Payment Card Industry Data Security Standard v3.2.1

Presented to: Sangoma US Inc. (USA) and Sangoma Technologies Inc. (Canada)

BID: 10060064

Date: 03-Apr-2024

Prepared by: David M Dennis

Viking Cloud Digitally signed by Viking Cloud Date: 2024.04.03 08:22:52 -05'00'

Version 052322

This page intentionally blank

Payment Card Industry (PCI)
Data Security Standard

Report on Compliance

PCI DSS v3.2.1 Template for Report on Compliance

Revision 1.0

June 2018

Document Changes

Date	Version	Description
February 2014	PCI DSS 3.0, Revision1.0	To introduce the template for submitting Reports on Compliance. *This document is intended for use with version 3.0 of the PCI Data Security Standard.*
July 2014	PCI DSS 3.0, Revision 1.1	Errata - Minor edits made to address typos and general errors, slight addition of content
April 2015	PCI DSS 3.1, Revision1.0	Revision to align with changes from PCI DSS 3.0 to PCI DSS 3.1 (see *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1* for details of those changes). Also includes minor edits made for clarification and/or format.
April 2016	PCI DSS 3.2, Revision 1.0	Revision to align with changes from PCI DSS 3.1 to PCI DSS 3.2 (see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2* for details of those changes). Also includes minor corrections and edits made for clarification and/or format.
June 2018	PCI DSS 3.2.1 Revision 1.0	Revision to align with changes from PCI DSS 3.2 to PCI DSS 3.2.1 (see *PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1* for details of changes). Also includes minor corrections and edits made for clarification and/or format.

Table of Contents

Introduction to the ROC Template

This document, the *PCI DSS Template for Report on Compliance for use with PCI DSS v3.2.1, Revision 1.0* ("ROC Reporting Template"), is the mandatory template for Qualified Security Assessors (QSAs) completing a Report on Compliance (ROC) for assessments against the *PCI DSS Requirements and Security Assessment Procedures v3.2.1.* The ROC Reporting Template provides reporting instructions and the template for QSAs to use. This can help provide reasonable assurance that a consistent level of reporting is present among assessors.

Use of this Reporting Template is mandatory for all v3.2.1 submissions.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase/decrease the number of rows, or to change column width. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as the report is written and for the recipient in understanding the context the responses and conclusions are made. Addition of text or sections is applicable within reason, as noted above. Refer to the "Frequently Asked Questions for use with ROC Reporting Template for PCI DSS v3.x" document on the PCI SSC website for further guidance.

The Report on Compliance (ROC) is produced during onsite PCI DSS assessments as part of an entity's validation process. The ROC provides details about the entity's environment and assessment methodology, and documents the entity's compliance status for each PCI DSS Requirement. A PCI DSS compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The ROC is effectively a ***summary of evidence*** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROC provides a comprehensive ***summary of testing activities performed and information collected*** during the assessment against the *PCI DSS Requirements and Security Assessment Procedures v3.2.1*. The information contained in a ROC must provide enough detail and coverage to verify that the assessed entity is compliant with all PCI DSS requirements.

ROC Sections

The ROC includes the following sections and appendices:

- Section 1: Contact Information and Report Date
- Section 2: Summary Overview
- Section 3: Description of Scope of Work and Approach Taken
- Section 4: Details about Reviewed Environment
- Section 5: Quarterly Scan Results
- Section 6: Findings and Observations

- Appendix A: Additional PCI DSS Requirements
- Appendices B and C: Compensating Controls and Compensating Controls Worksheet (as applicable)
- Appendix D: Segmentation and Sampling of Business Facilities/System Components (diagram)

The first five sections must be thoroughly and accurately completed, in order for the assessment findings in Section 6 and any applicable responses in the Appendices to have the proper context. The Reporting Template includes tables with Reporting Instructions built-in to help assessors provide all required information throughout the document. Responses should be specific, but efficient. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage. Parroting the testing procedure within a description is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is discouraged and details should be specifically relevant to the assessed entity.

ROC Summary of Assessor Findings

With the Reporting Template, an effort was made to efficiently use space, and as such, there is one response column for results/evidence ("ROC Reporting Details: Assessor's Response") instead of three. Additionally, the results for "Summary of Assessor Findings" were expanded to more effectively represent the testing and results that took place, which should be aligned with the Attestation of Compliance (AOC).

There are now five results possible – In Place, In Place with CCW (Compensating Control Worksheet), Not Applicable, Not Tested, and Not in Place. At each sub-requirement there is a place to designate the result ("Summary of Assessor Findings"), which can be checked as appropriate. See the example format on the following page, as referenced.

The following table is a helpful representation when considering which selection to make. Remember, only one response should be selected at the sub-requirement level, and reporting of that should be consistent with other required documents, such as the AOC.

Refer to the "Frequently Asked Questions for use with ROC Reporting Template for PCI DSS v3.x" document on the PCI SSC website for further guidance.

RESPONSE	WHEN TO USE THIS RESPONSE:	USING THE SAMPLE BELOW:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.	*In the sample, the Summary of Assessment Findings at 1.1 is "in place" if all report findings are in place for 1.1.a and 1.1.b or a combination of in place and not applicable.*

RESPONSE	WHEN TO USE THIS RESPONSE:	USING THE SAMPLE BELOW:
In Place w/ CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.	*In the sample, the Summary of Assessment Findings at 1.1 is "in place with CCW" if all report findings are in place for 1.1.a and 1.1.b with the use of a CCW for one or both (completed at the end of the report) or a combination of in place with CCW and not applicable.*
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.	*In the sample, the Summary of Assessment Findings at 1.1 is "not in place" if either 1.1.a or 1.1.b are concluded to be "not in place."*
N/A (Not Applicable)	The requirement does not apply to the organization's environment. All "not applicable" responses require reporting on testing performed to confirm the "not applicable" status. Note that a "Not Applicable" response still requires a detailed description explaining how it was determined that the requirement does not apply. In scenarios where the Reporting Instruction states, "If 'no/yes', mark as Not Applicable," assessors may simply enter "Not Applicable" or "N/A" and are not required to report on the testing performed to confirm the "Not Applicable" status. **Certain requirements are always applicable (3.2.1-3.2.3, for example), and that will be designated by a grey box under "Not Applicable."**	*In the sample, the Summary of Assessment Findings at 1.1 is "not applicable" if both 1.1.a and 1.1.b are concluded to be "not applicable." A requirement is applicable if any aspects of the requirement apply to the environment being assessed, and a "Not Applicable" designation in the Summary of Assessment Findings should not be used in this scenario.* ***Note, future-dated requirements are considered Not Applicable until the future date has passed. While it is true that the requirement is likely not tested (hence the original instructions), it is not required to be tested until the future date has passed, and the requirement is therefore not applicable until that date. As such, a "Not Applicable" response to future-dated requirements is accurate, whereas a "Not Tested" response would imply there was not any consideration as to whether it could apply (and be perceived as a partial or incomplete ROC).* *Once the future date has passed, responses to those requirements should be consistent with instructions for all requirements.*

RESPONSE	WHEN TO USE THIS RESPONSE:	USING THE SAMPLE BELOW:
Not Tested	The requirement (or any single aspect of the requirement) was not included for consideration in the assessment and was not tested in any way. (See "What is the difference between 'Not Applicable' and 'Not Tested'?" in the following section for examples of when this option should be used.)	*In the sample, the Summary of Assessment Findings at 1.1 is "not tested" if either 1.1.a or 1.1.b are concluded to be "not tested."*

What is the difference between "Not Applicable" and "Not Tested?"

Requirements that are deemed to be not applicable to an environment must be verified as such. Using the example of wireless and an organization that does not use wireless technology in any capacity, an assessor could select "N/A" for Requirements 1.2.3, 2.1.1, and 4.1.1, after the assessor confirms that there are no wireless technologies used in their CDE or that connect to their CDE via assessor testing. Once this has been confirmed, the organization may select "N/A" for those specific requirements, and the accompanying reporting must reflect the testing performed to confirm the not applicable status.

If a requirement is completely excluded from review without any consideration as to whether it could apply, the "Not Tested" option should be selected. Examples of situations where this could occur may include:

- An organization may be asked by their acquirer to validate a subset of requirements—for example: using the prioritized approach to validate certain milestones.
- An organization may wish to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption methodology that requires assessment of PCI DSS Requirements 2, 3, and 4.
- A service provider organization might offer a service that covers only a limited number of PCI DSS requirements—for example, a physical storage provider may only wish to validate the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization only wishes to validate certain PCI DSS requirements even though other requirements might also apply to their environment. Compliance is determined by the brands and acquirers, and the AOCs they see will be clear in what was tested and not tested. They will decide whether to accept a ROC with something "not tested," and the QSA should speak with them if any exception like this is planned. This should not change current practice, just reporting.

Requirement X: Sample

Note – checkboxes have been added to the "Summary of Assessment Findings" so that the assessor may double click to check the applicable summary result. Hover over the box you'd like to mark and click once to mark with an 'x'. To remove a mark, hover over the box and click again.

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.1 Sample sub-requirement			☐	☐	☐	☐	☐
1.1.a Sample testing procedure	Reporting Instruction	*<Report Findings Here>*					
1.1.b Sample testing procedure	Reporting Instruction	*<Report Findings Here>*					

ROC Reporting Details

The reporting instructions in the Reporting Template explain the intent of the response required. There is no need to repeat the testing procedure or the reporting instruction within each assessor response. As noted earlier, responses should be specific and relevant to the assessed entity. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage and should avoid parroting of the testing procedure without additional detail or generic template language.

Assessor responses will generally fall into categories such as the following:

- One word **(yes/no)**

  Example Reporting Instruction: ***Indicate whether*** *the assessed entity is an issuer or supports issuing services.* ***(yes/no)***

- Document name or interviewee job title/reference – In Sections 4.9, "Documentation Reviewed," and 4.10, "Individuals Interviewed" below, there is a space for a reference number and ***it is the QSA's choice*** to use the document name/interviewee job title or the reference number at the individual reporting instruction response.

  Example Reporting Instruction: ***Identify*** *the document that defines vendor software development processes.*
  Example Reporting Instruction: ***Identify the individuals*** *interviewed who confirm that …*

- Sample description – For sampling, the QSA must use the table at "Sample sets for reporting" in the Details about Reviewed Environment section of this document to fully report the sampling, but ***it is the QSA's choice*** to use the Sample set reference number ("Sample Set-5") or list out the items from the sample again at the individual reporting instruction response. If sampling is not used, then the types of components that were tested must still be identified in Section 6 Findings and Observations. This may be accomplished by either using Sample Set Reference numbers or by listing the tested items individually in the response.

  Example Reporting Instruction: ***Identify the sample*** *of removable media observed.*

- Brief description/short answer – Short and to the point, but provide detail and individual content that is not simply an echoing of the testing procedure or reporting instruction nor a template answer used from report-to-report, but instead relevant and specific to the assessed entity. These responses must include unique details, such as the specific system configurations reviewed (to include what the assessor observed in the configurations) and specific processes observed (to include a summary of what was witnessed and how that verified the criteria of the testing

procedure). It is not enough to simply state that it was verified. Responses must go beyond that and include details regarding *how* a requirement is in place.

Example Reporting Instruction: ***Describe*** *the procedures for secure key distribution that were observed to be implemented.*
Example Reporting Instruction: For the interview, ***summarize the relevant details*** *discussed that verify …*

Dependence on another service provider's compliance:

Generally, when reporting on a requirement where a third-party service provider is responsible for the tasks, an acceptable response for an "in place" finding may be something like:

"Assessor verified this is the responsibility of Service Provider X, as verified through review of x/y contract (document). Assessor reviewed the AOC for Service Provider X, dated MM/DD/YYYY, and confirmed the service provider was found to be PCI DSS compliant ***against PCI DSS v3.2 (or PCI DSS v3.2.1)*** *for all applicable requirements, and that it covers the scope of the services used by the assessed entity."*

That response could vary, but what's important is that it is noted as "in place" and that there has been a level of testing by the assessor to support the conclusion that this responsibility is verified and that the responsible party has been tested against the requirement and found to be compliant.

Do's and Don'ts: Reporting Expectations

DO:	*DON'T:*
▪ Use this Reporting Template when assessing against v3.2.1 of the PCI DSS. ▪ Complete all sections in the order specified. ▪ Read and understand the intent of each Requirement and Testing Procedure. ▪ Provide a response for every Testing Procedure. ▪ Provide sufficient detail and information to support the designated finding, but be concise. ▪ Describe *how* a Requirement is in place per the Reporting Instruction, not just that it *was* verified. ▪ Ensure the parts of the Testing Procedure and Reporting Instruction are addressed. ▪ Ensure the response covers all applicable system components. ▪ Perform an internal quality assurance review of the ROC for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don't report items in the "In Place" column unless they have been verified as being "in place" as stated. ▪ Don't include forward-looking statements or project plans in the "In Place" assessor response. ▪ Don't simply repeat or echo the Testing Procedure in the response. ▪ Don't copy responses from one Testing Procedure to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment. ▪ Don't leave any spaces blank. If a section does not apply, annotate it as such.

ROC Template for PCI Data Security Standard v3.2.1

This template is to be used for creating a Report on Compliance. Content and format for a ROC is defined as follows:

1. Contact Information and Report Date

1.1 Contact information

Client	
▪ Company name:	Sangoma US Inc. (USA) and Sangoma Technologies Inc. (Canada)
▪ Company address:	Sangoma US Inc. 301 N Cattlemen Rd, Suite 300 Sarasota, FL, USA 34232 Sangoma Technologies Inc. 100 Renfrew Dr., Suite 100 Markham, ON, CA L3R 9R6
▪ Company URL:	https://www.sangoma.com
▪ Company contact name:	Eric Krichbaum
▪ Contact phone number:	+1 (941) 234-0001 (USA) +1 (905) 474-1990 (Canada)
▪ Contact e-mail address:	ekrichbaum@sangoma.com
Assessor Company	
▪ Company name:	VikingCloud
▪ Company address:	70 W Madison St., Suite 400, Chicago IL 60602 USA
▪ Company website:	https://www.vikingcloud.com
Assessor	
▪ Lead Assessor name:	David M Dennis
▪ Assessor PCI credentials: (QSA, PA-QSA, etc.)	QSA
▪ Assessor phone number:	+1 (833) 907-0702
▪ Assessor e-mail address:	daviddennis@vikingcloud.com
▪ List all other assessors involved in the assessment. If there were none, mark as Not Applicable. (add rows as needed)	
Assessor name:	Assessor PCI credentials: (QSA, PA-QSA, etc.)
Not Applicable	Not Applicable
▪ List all Associate QSAs involved in the assessment. If there were none, mark as Not Applicable. (add rows as needed)	

Associate QSA name:	Associate QSA mentor name:
Not Applicable	Not Applicable
Assessor Quality Assurance (QA) Primary Reviewer for this specific report (not the general QA contact for the QSA)	
▪ QA reviewer name:	Scott Frazier
▪ QA reviewer phone number:	+1 (833) 907-0702
▪ QA reviewer e-mail address:	compliance-qa@vikingcloud.com

1.2 Date and timeframe of assessment

▪ Date of Report:	03-Apr-2024
▪ Timeframe of assessment (start date to completion date):	19-Jan-2024 to 8-Mar-2024
▪ Identify date(s) spent onsite at the entity:	Due to Sangoma relying on 100% remote workers except for the Seattle data center site, virtual interviews and live demonstrations occurred on 19-Jan-2024 and 22-Jan-2024. On-site at the Seattle data center colocation facility occurred on 24-Jan-2024.
▪ Describe the time spent onsite at the entity, time spent performing remote assessment activities and time spent on validation of remediation activities.	From 19-Jan-2024 to 22-Jan-2024, remote meetings were held between QSA and Sangoma compliance and project management to plan assessment interviews, confirm evidence-gathering requests, for a total of 5 days. Remote document review occurred from 19-Jan-2024, through 17-Feb-2024 for a total of five days. Live remote demonstrations of working processes and network sampling occurred Systems Administrators, Security Engineers, Chief Security Officer, Turn-up and TAC employees, HR employee, and data center employees on 19-Jan-2024, and 22-Jan-2024, for a total of 2 days. Topics covered firewalls, routers, switches, network provisioning, customer provisioning and access, central logging, intrusion detection, server provisioning, patching, and upgrading, as well as penetration testing, scanning, intrusion detection, anti-virus and file integrity monitoring. In-person data center review involving on-site data center walk-through and interview with Lunavi site representative (Int-10) in Seattle occurred on 24-Jan-2024, for one day. Follow-up remediation, evidence review, and document review occurred from 19-Jan-2024, through 17-Feb-2024, for a total of 8 days. Final report drafting occurred from 12-Feb-2024, until 8-Mar-2024, for a total of 12 days.

1.3 PCI DSS version

▪ Version of the PCI Data Security Standard used for the assessment (should be 3.2.1):	3.2.1

1.4 Additional services provided by QSA company

The PCI SSC Qualification Requirements for Qualified Security Assessors (QSA) v3.0 includes content on "Independence," which specifies requirements for assessor disclosure of services and/or offerings that could reasonably be viewed to affect independence of assessment. Complete the below after review of relevant portions of the Qualification Requirements document(s) to ensure responses are consistent with documented obligations.

▪ Disclose all services offered to the assessed entity by the QSAC, including but not limited to whether the assessed entity uses any security-related devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights or that the QSA has configured or manages:	VikingCloud provides ASV External Scanning (Requirement 11.2) VikingCloud provides Internal and External Penetration Testing (Requirement 11.3). VikingCloud has a professional agreement to provide services relating to PCI-DSS activities where appropriate.
▪ Describe efforts made to ensure no conflict of interest resulted from the above mentioned services provided by the QSAC:	No conflict of interest exists, as VikingCloud QSA plays no role in VikingCloud ASV scanning process and has no access to VikingCloud ASV scans or VikingCloud Penetration Tests until Sangoma shares the scans or testing reports with QSA. As QSA, I had no involvement in delivering these scanning services provided by VikingCloud, or penetration testing services provided by VikingCloud on behalf of Sangoma.

1.5 Summary of Findings

PCI DSS Requirement	Summary of Findings (check one)			
	Compliant	Non-Compliant	Not Applicable	Not Tested
1. Install and maintain a firewall configuration to protect cardholder data	☒	☐	☐	☐
2. Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	☐	☐
3. Protect stored cardholder data	☒	☐	☐	☐
4. Encrypt transmission of cardholder data across open, public networks	☒	☐	☐	☐
5. Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	☐	☐
6. Develop and maintain secure systems and applications	☒	☐	☐	☐
7. Restrict access to cardholder data by business need to know	☒	☐	☐	☐
8. Identify and authenticate access to system components	☒	☐	☐	☐
9. Restrict physical access to cardholder data	☒	☐	☐	☐
10. Track and monitor all access to network resources and cardholder data	☒	☐	☐	☐
11. Regularly test security systems and processes	☒	☐	☐	☐
12. Maintain a policy that addresses information security for all personnel	☒	☐	☐	☐
Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	☒	☐
Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections	☐	☐	☒	☐
Appendix A3: Designated Entities Supplemental Validation	☐	☐	☒	☐

2. Summary Overview

2.1 Description of the entity's payment card business

Provide an overview of the entity's payment card business, including:

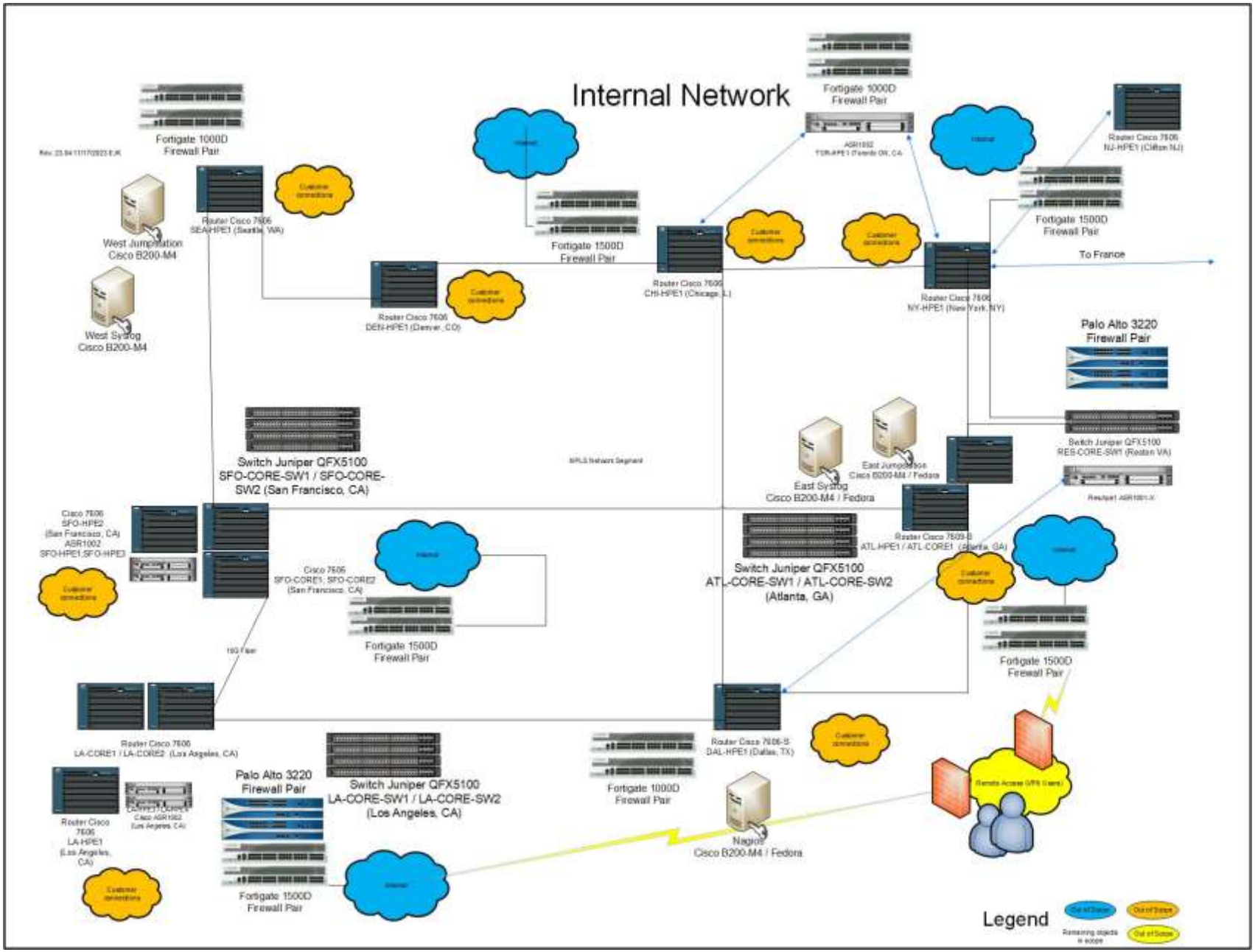
▪ Describe the nature of the entity's business (what kind of work they do, etc.) ***Note:*** *This is not intended to be a cut-and-paste from the entity's website, but should be a tailored description that shows the assessor understands the business of the entity being assessed.*	Sangoma US Inc. (USA) and Sangoma Technologies Inc. (Canada), collectively for this report known as Sangoma, a Level 1 Service Provider, provides telecommunications, internet routing, and various "as a Service" services to its customers; business voice over IP, SIP trunking, video meeting services, contact center services, team hub services, studio applications, and network services. Sangoma does not store, process, or transmit cardholder data (PIN/PAN) or healthcare information (PHI). As the communications interface between complying merchants and service providers and their acquiring banks or other intermediaries, Sangoma requires the compliance of its routing infrastructure, and specific products. Business Voice (UCaaS), SIP Trunking (TaaS), Contact Center (CCaaS), Video Meeting (VMaaS), Studio Apps (CPaaS), Teamhub (ColaaS), and network services (NaaS, SaaS) are included.
▪ Describe how the entity stores, processes, and/or transmits cardholder data. ***Note:*** *This is not intended to be a cut-and-paste from above, but should build on the understanding of the business and the impact this can have upon the security of cardholder data.*	Sangoma does not accept any cardholder data, does not store cardholder data. Sangoma acts as a service provider for its customers for networking and data transport and has no visibility into any cardholder data that its customers might store, process or transmit. The employees of Sangoma do not interact with cardholder data in any aspect of management of these environments. The management and support of the customer networks is in scope for Sangoma, as well as procedures and network architecture followed to separate administrative from customer networks. PCI-compliant handling of customer premesis equipment (CPE), "turn-up procedures" and support of the devices in the field is also included.
▪ Describe why the entity stores, processes, and/or transmits cardholder data. ***Note:*** *This is not intended to be a cut-and-paste from above, but should build on the understanding of the business and the impact this can have upon the security of cardholder data.*	Sangoma has a role as network provider, which means that it has no responsibility for cardholder data that its customers potentially could transmit. It's access to network devices could impact the security of CHD belonging to their customers, if its customers are using the network for CHD transmission.
▪ Identify the types of payment channels the entity serves, such as card-present and card-not-present (for example, mail order/telephone order (MOTO), e-commerce).	**Card-Present:** • Sangoma does not accept Card-Present transactions **Card-Not-Present:** • Sangoma does not accept Card-Not-Present transactions **PIN/debit:** • Sangoma does not accept PIN/Debit transactions

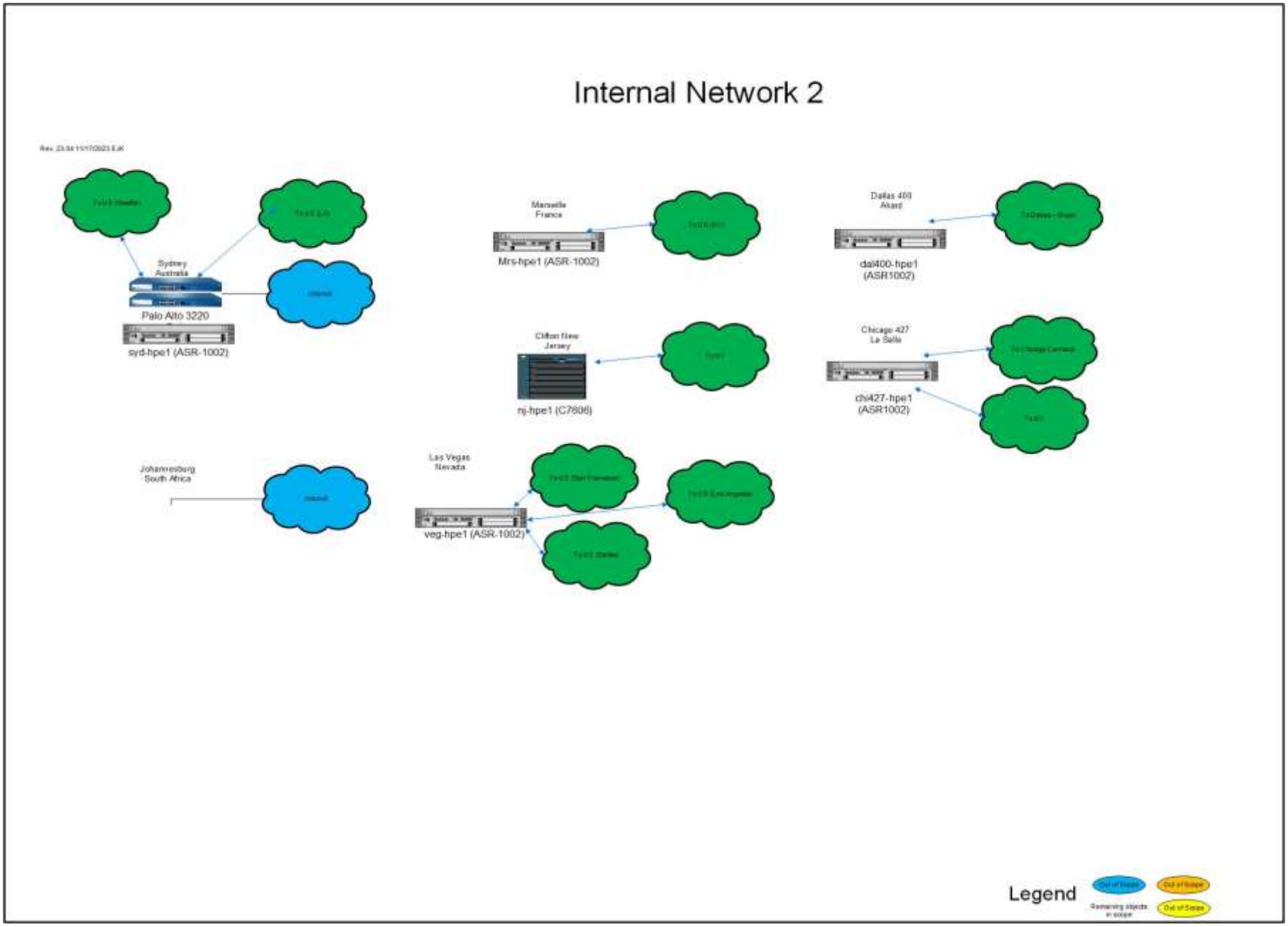
▪ Other details, if applicable:	Not Applicable

2.2 High-level network diagram(s)

Provide a ***high-level*** network diagram (either obtained from the entity or created by assessor) of the entity's networking topography, showing the overall architecture of the environment being assessed. This high-level diagram should summarize all locations and key systems, and the boundaries between them and should include the following:

- Connections into and out of the network including demarcation points between the cardholder data environment (CDE) and other networks/zones
- Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
- Other necessary payment components, as applicable





3. Description of Scope of Work and Approach Taken

3.1 Assessor's validation of defined cardholder data environment and scope accuracy

Document how the assessor validated the accuracy of the defined CDE/PCI DSS scope for the assessment, including:

As noted in PCI DSS, v3.2.1 – "At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or if compromised could impact the CDE (e.g. authentication servers) to ensure they are included in the PCI DSS scope." *Note – additional reporting has been added below to emphasize systems that are connected to or if compromised could impact the CDE.*	
▪ Describe the methods or processes (for example, the specific types of tools, observations, feedback, scans, data flow analysis) used to identify and document all existences of cardholder data (as executed by the assessed entity, assessor or a combination):	Throughout the year, Sangoma used ongoing assessment of risk by the Information Security Officer and followed the Sangoma risk-management process. This risk management process included network design review and regular firewall review activity with senior technical staff. Tools used include Nessus for network boundary rules testing. Sangoma business also regularly consults the Security Officer on matters relating to business onboarding, and includes any risk potential to the company. This activity I found met the criteria for an effort that met compliance goals, and that the scope that resulted was accurate and complete.
▪ Describe the methods or processes (for example, the specific types of tools, observations, feedback, scans, data flow analysis) used to verify that no cardholder data exists outside of the defined CDE (as executed by the assessed entity, assessor or a combination):	Sangoma' Information Security Officer and risk management process determines by interview with business owners and managers in Sangoma' business, by internal scan using Nessus internal scanner and by risk management review (Int-1, Int-3) that no internal storage for CHD, as well as no business case for storing CHD exists. I used interviews, a review of the current Risk Assessment, and a review of the out-of-scope environment, and the controls that separate these, to confirm that the environment, which contains no CHD was defined according to documentation provided. I concluded that the scope was accurate from these activities.
▪ Describe how the results of the methods/processes were documented (for example, the results may be a diagram or an inventory of cardholder data locations):	The results of Sangoma' process was to update their Network diagrams (Doc-42, Doc-43, Doc-44), device configuration (Sample Set-1, Sample Set-2, Sample Set-20), and device configuration snapshots (Sample Set-1, Sample Set-2, Sample Set-4, Sample Set-5).
▪ Describe how the results of the methods/processes were evaluated by the assessor to verify that the PCI DSS scope of review is appropriate: ***Note** – the response must go beyond listing the activities that the assessor performed to evaluate the results of the methods/processes; the assessor must also include details regarding the results of the outcome of those activities that gave the assessor the level of assurance that the scope is appropriate.*	I conducted specific interviews by remote Zoom session with Int-1 and Int-2 that covered the Sangoma network architecture, and the placement of systems within those networks. I conducted specific interviews with Int-1 and Int-2 who demonstrated Sample Set-1 that covered the Sangoma network architecture, and the placement of systems within those networks. With a sampling of systems and servers, I identified Sangoma' operating system platforms, network placement, access controls, and security controls that transmit customer data. The assessment also included interviews, where I saw that processes were being followed as documented, and procedures

	were known to technical employees. I observed that documents were updated on an ongoing basis throughout the year by the compliance team. I observed that these included ongoing review of PCI-DSS scope. This enabled me to determine that the risk activities were thorough.
▪ Describe why the methods (for example, tools, observations, feedback, scans, data flow analysis, or any environment design decisions that were made to help limit the scope of the environment) used for scope verification are considered by the assessor to be effective and accurate:	After interviews with Sangoma' employees, I observed that the processes used were thorough and follow a "business as usual" method, which means the following: • Sangoma builds compliance-related activities into their day-to-day operations. • Documents are updated on an ongoing basis, and scoping activity is conducted every time a process that could impact the security of the cardholder environment is changed or considered for a business-driven change in some way. This approach is documented by Sangoma policies. In my judgment, the professional and thorough process used have resulted in an effective and accurate scope determination.
▪ Provide the name of the assessor who attests that the defined CDE and scope of the assessment has been verified to be accurate, to the best of the assessor's ability and with all due diligence:	David M Dennis
▪ Other details, if applicable:	Not Applicable

3.2 Cardholder Data Environment (CDE) overview

Provide an overview of the cardholder data environment encompassing the people, processes, technologies, and locations (for example, client's Internet access points, internal corporate network, processing connections).

▪ People – such as technical support, management, administrators, operations teams, cashiers, telephone operators, physical security, etc.: ***Note** – this is not intended to be a list of individuals interviewed, but instead a list of the types of people, teams, etc. who were included in the scope.*	• Operations Staff • Customer Support Users • Network Host Business
▪ Processes – such as payment channels, business functions, etc.:	▪ Customer onboarding process ▪ Customer support process ▪ Self-audit process ▪ Employee training process ▪ Change control process ▪ Server management ▪ Network management

▪ Technologies – such as e-commerce systems, internal network segments, DMZ segments, processor connections, POS systems, encryption mechanisms, etc.: ***Note*** *– this is not intended to be a list of devices but instead a list of the types of technologies, purposes, functions, etc. included in the scope.*	▪ Firewalls ▪ Routers ▪ Virtual Customer Environments ▪ Switches ▪ Administrative Servers ▪ Logging Solutions ▪ File Integrity Monitoring ▪ VPN ▪ Authentication Services ▪ Production Network ▪ Workstations
▪ Locations/sites/stores – such as retail outlets, data centers, corporate office locations, call centers, etc.:	Data Center, Seattle, WA, USA (in scope, visited, non-AOC) Data Center (CoreSite), Los Angeles, CA, USA (in scope, not visited, validated by AoC review). Data Center (Digital Reality), New York, NY, USA (in scope, not visited, validated by AoC review). Data Center (CoreSite), Atlanta, GA, USA (in scope, not visited, validated by AoC review). Data Center (Digital Reality), Atlanta, GA, USA (in scope, not visited, validated by AoC review). Data Center (Digital Reality), Dallas, TX, USA (in scope, not visited, validated by AoC review). Data Center (CoreSite), Chicago, IL, USA (in scope, not visited, validated by AoC review). Data Center (Equinox), Chicago, IL, USA (in scope, not visited, validated by AoC review). Data Center (Digital Reality), Clifton, NJ, USA (in scope, not visited, validated by AoC review). Data Center (CoreSite), Denver, CO, USA (in scope, not visited, validated by AoC review). Data Center (Switch), Las Vegas, NV, USA (in scope, not visited, validated by AoC review). Data Center (Digital Reality), San Francisco, CA, USA (in scope, not visited, validated by AoC review). Data Center (Equinox), Toronto, ON, Canada (in scope, not visited, validated by AoC review).

	Data Center (CoreSite), Reston, VA, USA (in scope, not visited, validated by AoC review). Data Center (Equinox), Sydney, NSW, Australia (in scope, not visited, validated by AoC review). Data Center (Digital Reality), (not in scope for data, in scope for remote access, not visited) Marseille, France Data Center (Digital Reality), Johannesburg, South Africa (not in scope for data, in scope for remote access, not visited, non-AoC).
▪ Other details, if applicable:	Due to Sangoma's policy to move to all-remote workers, live-remote review of non-AOC facilities were conducted with employees during live Zoom sessions with assistance from data center employees for these sites. In all cases, steps were taken to meet the rigor and intent of an actual onsite assessment, and therefore not compromise the integrity of the assessment when interviewing remotely. These steps taken included: • Video and screen capture of evidence from live sessions, when permitted by policy; • Live Q and A during Zoom meeting included live evidence reviews, to simulate in-person review, when permitted by policy. Sangoma makes use of CoreSite data center facilities in Atlanta, GA, USA; Reston, VA, USA; Los Angeles, CA (2), USA; Chicago, IL, USA; and Denver, CO, USA. I read Doc-30 to confirm requirements provided by these data centers, and which are provided by Sangoma. I read Doc-14 which tracked which requirements are provided by the data centers with AoCs, and compared those with AoC obtained for CoreSite and found that Sangoma uses CoreSite for requirements which the service provider has been found to be compliant by review of the AoC, PCI-DSS v3.2.1, date 30 Jun 2023 (Doc-22). I validated the compliance of these sites by review of AoC and observed CoreSite is compliant with these PCI-DSS v3.2.1 requirements: Req. 9.1, Req. 9.2, Req. 9.3, Req. 9.4, I read Doc-14 and Doc-30 to observe that Sangoma is responsible for: Req. 9.5.

	I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma. I validated the compliance of these PCI-DSS v3.2.1 requirements of Lunavi by live remote Zoom site visit with Int-1 and on-site interview with Int-10, following a live-walkaround script and live instructions given, to observe camera positions, data center sign-in, doorway multi-factor authentication, badging, sign-in and out, exit door position and camera, Sangoma equipment row and camera, position of data destruction and any consoles, wall jacks and cage boundaries, to observe that Lunavi is compliant with these requirements: Data Center provider Lunavi is responsible in Seattle for the following PCI-DSS v3.2.1 Requirements for Sangoma: Req. 9.1, Req. 9.2, Req. 9.3, Req. 9.4. Sangoma makes use of Digital Realty data center facilities in Atlanta, GA, USA; Clifton, NJ, USA; Dallas, TX, USA; San Francisco, CA, USA; Chicago, IL, USA; Marseilles, FR; New York, NY, USA; Johannesburg, South Africa. I read Doc-30 to confirm requirements provided by these data centers, and which are provided by Sangoma. I read Doc-14 which tracked which requirements are provided by the data centers with AoCs and compared those with AoC obtained for Digital Realty and found that Sangoma uses Digital Realty for requirements which the service provider have been found to be compliant, PCI-DSS v3.2.1, AoC date 28 Feb 2023 (Doc-45). I validated the compliance of these sites by review of AoC and observed Digital Realty is compliant with these PCI-DSS v3.2.1 requirements: Req. 9.1, Req. 9.2, Req. 9.3, and Req. 9.4. I read Doc-30 to observe that Sangoma is responsible for Req. 9.5 Sangoma makes use of Equinix data center facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada.

	I read Doc-30 to confirm requirements provided by these data centers, and which are provided by Sangoma. I read Doc-14 which tracked which requirements are provided by the data centers with AoCs and compared those with AoC obtained for Equinix and found that Sangoma uses Equinix for requirements which the service provider have been found to be compliant, PCI-DSS v3.2.1, AoC dated 5 Nov 2023 (Doc-9). I validated the compliance of these sites by review of AoC and observed Equinix is compliant with these PCI-DSS v3.2.1 requirements: Req. 9.1, Req. 9.2, Req. 9.3, and Req. 9.4. I read Doc-30 to observe that Sangoma is responsible for Req. 9.5.

3.3 Network segmentation

▪ Identify whether the assessed entity has used network segmentation to reduce the scope of the assessment. **(yes/no)** ***Note*** *-- An environment with no segmentation is considered a "flat" network where all systems are considered in scope due to a lack of segmentation.*	yes
▪ ***If segmentation is not used:*** Provide the name of the assessor who attests that the whole network has been included in the scope of the assessment.	Not Applicable
▪ ***If segmentation is used:*** Briefly describe how the segmentation is implemented.	Segmentation is implemented using router ACL and firewall rules sets under control of Sangoma policies to create strict separation between customer networks and Sangoma administrative network employee access.
– Identify the technologies used and any supporting processes	Segmentation is provided by Cisco 7606-S, Cisco 7609-S and Cisco 7606 routers. Traffic is limited by FortiNet FortiGate 1500D firewalls to only defined IP ranges in these networks. All devices are managed by Sangoma, using Sangoma-approved and deployed hardened images, based off SANS and Cisco best-practices guidance. Traffic is monitored by OSSEC host-based IDS running on the Fedora Linux hosts, and alerted by Logwatch for any traffic that is outside defined segments. Authentication is provided by TACACS+ managed by Sangoma for their devices, which are accessed using OpenSSH for a secure connection remotely.
– Explain how the assessor validated the effectiveness of the segmentation, as follows:	
– Describe the methods used to validate the effectiveness of the segmentation (for example, observed configurations of implemented technologies, tools used, network traffic analysis, etc.).	Through observation of the firewall rule sets, through discussion with Sangoma management and Subject Matter Experts (SMEs) and review of the network and data flow diagrams, I verified that network environments are not allowed to freely communicate beyond segmentation points. In

	addition, I observed a failed attempt to access outside of the defined customer in-scope environment.
– Describe how it was verified that the segmentation is functioning as intended ***Note –*** *the response must go beyond listing the activities that the assessor performed and must provide specific details regarding how segmentation is functioning as intended.*	I observed through visual inspection of rules on all technology pieces matched with knowledge of firewall and VLAN configuration during a live Zoom session. I interviewed Int-1 and Int-2 who were able to describe network segmentation as implemented at Sangoma. I observed by scan reports to changes (Sample Set-10) performed on the network and found that Sangoma's network was tested by Sangoma network team, and that the segmentation was functioning as intended. I also reviewed firewall rules (Sample Set-1) and compared those to Doc-15 and Doc-21 and found that the implementation matched the descriptions provided, using vendor recommended best practices where appropriate for Sangoma' network.
– Identify the security controls that are in place to ensure the integrity of the segmentation mechanisms (e.g., access controls, change management, logging, monitoring, etc.).	Fortinet FortiGate firewalls and Cisco routers are used to provide a fully segmented environment for Sangoma customers. Rsyslog centralized logging is used, and Logwatch is used to log any potential incident of unauthorized access and alert appropriate personnel. I observed that penetration is used to test internal and external boundaries, and that specific procedures are in place so that no unauthorized changes to the network may occur. Senior level approval for any network change must be given, and access to network equipment is limited by MFA, TACACS+ authentication, and tightly controlled access lists.
– Describe how it was verified that the identified security controls are in place ***Note*** *– the response must go beyond listing the activities that the assessor performed and must provide specific details of what the assessor observed to get the level of assurance that the identified security controls are in place.*	All changes to the Sangoma environment must go through review and approval by Int-1 and Int-2, including any change to logging, monitoring, and access controls. I observed this process by review of firewall and router changes and found that only Int-1 is allowed to approve them. I observed strict access list of who may log into the network is maintained by Int-1 and Int-4, and that this list may not be added to without senior level permission and an audit trail being created. I observed this maintains the integrity of the segmentation controls. Additionally, access to the controlled environment is limited to only those in possession of root-level access to networking devices.
▪ Provide the name of the assessor who attests that the segmentation was verified to be adequate to reduce the scope of the assessment AND that the technologies/processes used to implement segmentation were included in the PCI DSS assessment.	David M Dennis

3.4 Network segment details

Describe all networks that store, process and/or transmit CHD:

Network Name (in scope)	Function/ Purpose of Network
Not Applicable	Not Applicable. No network in the Sangoma environment stores, processes or transmits CHD.

Describe all networks that do not store, process and/or transmit CHD, but are still in scope (e.g., connected to the CDE or provide management functions to the CDE):

Network Name (in scope)	Function/ Purpose of Network
ATL-HPE1	Hosted provider edge – connects customer network to transport network
ATL-CORE1	Hosted Provider Core Network
ATL-CORE-SW1	Hosted Provider Core Network
ATL-CORE-SW2	Hosted Provider Core Network
NY-HPE1	Hosted provider edge – connects customer network to transport network
Res-hpe1	Hosted provider edge – connects customer network to transport network
RES-CORE-SW1	Hosted Provider Core Network
LA-CORE-SW1	Hosted Provider Core Network
LA-CORE-SW2	Hosted Provider Core Network
TOR-HPE1	Hosted provider edge – connects customer network to transport network
CHI-HPE1	Hosted provider edge – connects customer network to transport network
DEN-HPE1	Hosted provider edge – connects customer network to transport network
SEA-HPE1	Hosted provider edge – connects customer network to transport network
SJC-HPE1	Hosted provider edge – connects customer network to transport network
SFO-CORE1	Hosted Provider Core Network
SFO-CORE2	Hosted Provider Core Network
SFO-CORE-SW1	Hosted Provider Core Network

SFO-CORE-SW2	Hosted Provider Core Network
SFO-HPE1	Hosted provider edge – connects customer network to transport network
SFO-HPE2	Hosted provider edge – connects customer network to transport network
SFO-HPE3	Hosted provider edge – connects customer network to transport network
LA-CORE1	Hosted Provider Core Network
LA-CORE2	Hosted Provider Core Network
nj-hpe1	Hosted Provider Core Network
LA-HPE1	Hosted provider edge – connects customer network to transport network
LA-HPE2	Hosted provider edge – connects customer network to transport network
LA-HPE2	Hosted provider edge – connects customer network to transport network
LA-HPE4	Hosted provider edge – connects customer network to transport network
DAL-HPE1	Hosted provider edge – connects customer network to transport network
veg-hpe1	Hosted provider edge – connects customer network to transport network
syd-hpe1	Hosted provider edge – connects customer network to transport network
Mrs-hpe1	Hosted provider edge – connects customer network to transport network
Johannesburg South Africa	Hosted provider edge – connects customer network to transport network

Describe any networks confirmed to be out of scope:

Network Name (out of scope)	**Function/ Purpose of Network**
Customer Connections	Customer Connections contained in FortiNet VDOM (Virtual Domains)
Remote Access (VPN Users)	Origin networks of administrative access, prior to firewall, which includes Offices of Sangoma / remote access employees.

3.5 Connected entities for payment processing and transmission

Complete the following for connected entities for processing and/or transmission. If the assessor needs to include additional reporting for the specific brand and/or acquirer, it can be included either here within 3.5 or as an appendix at the end of this report. Do not alter the Attestation of Compliance (AOC) for this purpose.

Identify All Processing and Transmitting Entities (i.e. Acquirer/ Bank/ Brands)	Directly Connected? (yes/no)	Reason(s) for Connection:		Description of any discussions/issues between the QSA and Processing Entity on behalf of the Assessed Entity for this PCI DSS Assessment (if any)
		Processing	Transmission	
Not Applicable	Not Applicable	☐	☐	Not Applicable

▪ Other details, if applicable (add content or tables here for brand/acquirer use, if needed):	Sangoma is not an acquirer. Sangoma is not an issuer. Sangoma does not perform ATM driving functions. Sangoma does not have any direct card brand connections. Sangoma is not a VisaNet processor. Sangoma does not use any off-site media storage. Sangoma uses virtualization (FortiNet VDOM) for its customer-facing environments. Sangoma is not using a P2PE solution in the CDE. Sangoma is not using an E2EE solution in the CDE.

3.6 Other business entities that require compliance with the PCI DSS

Entities wholly owned by the assessed entity that are required to comply with PCI DSS:
(This may include subsidiaries, different brands, DBAs, etc.)

Wholly Owned Entity Name	Reviewed:	
	As part of this assessment	Separately
No wholly owned entities	Not Applicable	Not Applicable

International entities owned by the assessed entity that are required to comply with PCI DSS:

List all countries where the entity conducts business. (If there are no international entities, then the country where the assessment is occurring should be included at a minimum.)	Country
	United States
	Canada
	France
	South Africa

	Australia

International Entity Name	Facilities in this country reviewed:	
	As part of this assessment	Separately
No international entities owned	Not Applicable	Not Applicable

3.7 Wireless summary

▪ Indicate whether there are wireless networks or technologies in use (in or out of scope), **(yes/no)**	no
If "no," describe how the assessor verified that there are no wireless networks or technologies in use.	I observed by review of PCI Inventory (Doc-14) that there are no wireless devices in use.
*If "yes," indicate whether wireless is in scope (i.e. part of the CDE, connected to or could impact the security of the cardholder data environment), **(yes/no)**:* This would include: – Wireless LANs – Wireless payment applications (for example, POS terminals) – All other wireless devices/technologies	Not Applicable

3.8 Wireless details

For each wireless technology in scope, identify the following:

Identified wireless technology	For each wireless technology in scope, identify the following (yes/no):		
	Whether the technology is used to store, process or transmit CHD	Whether the technology is connected to or part of the CDE	Whether the technology could impact the security of the CDE
Not Applicable	Not Applicable	Not Applicable	Not Applicable

Wireless technology not in scope for this assessment:

Identified wireless technology (not in scope)	Describe how the wireless technology was validated by the assessor to be not in scope
Not Applicable	Not Applicable

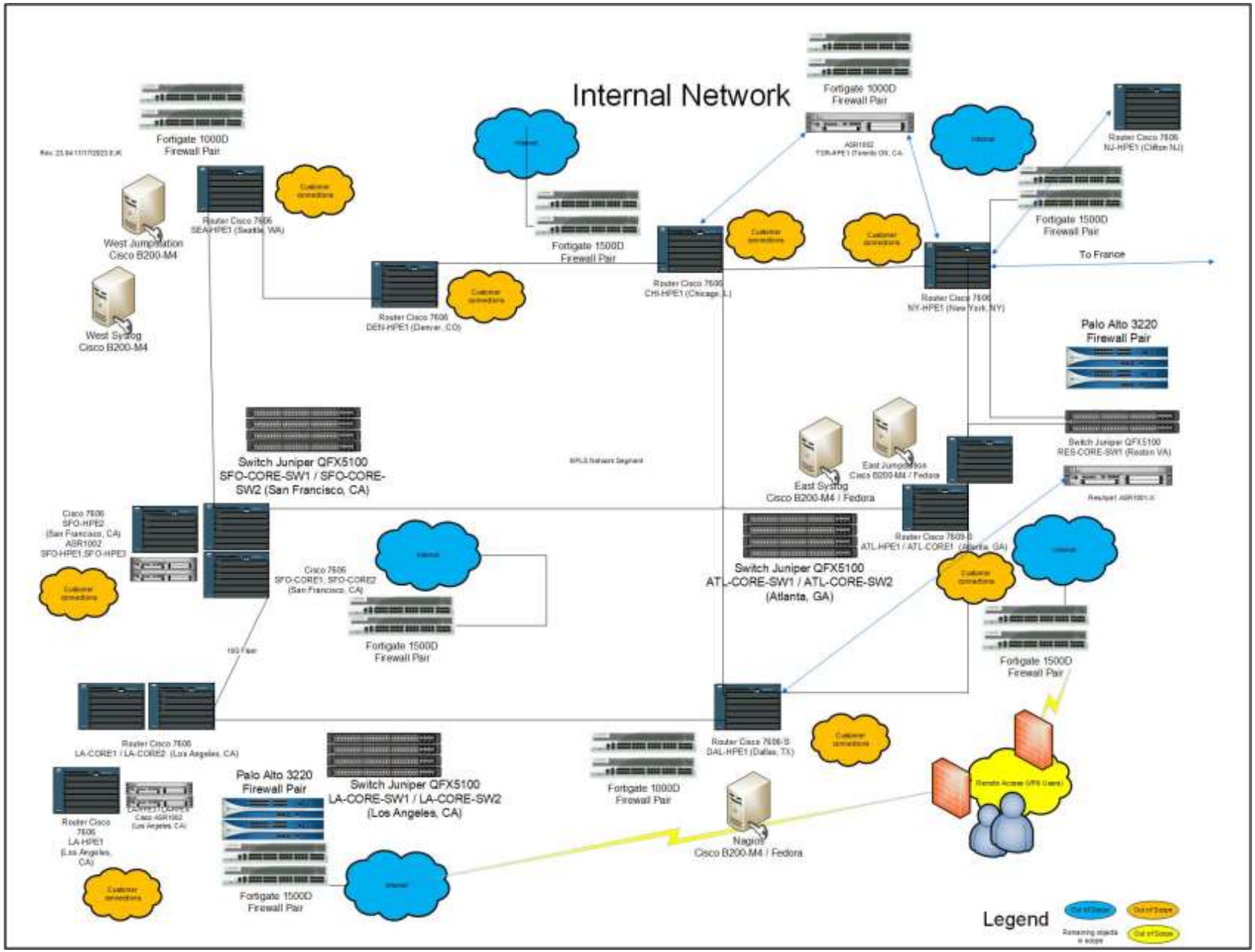
4. Details about Reviewed Environment

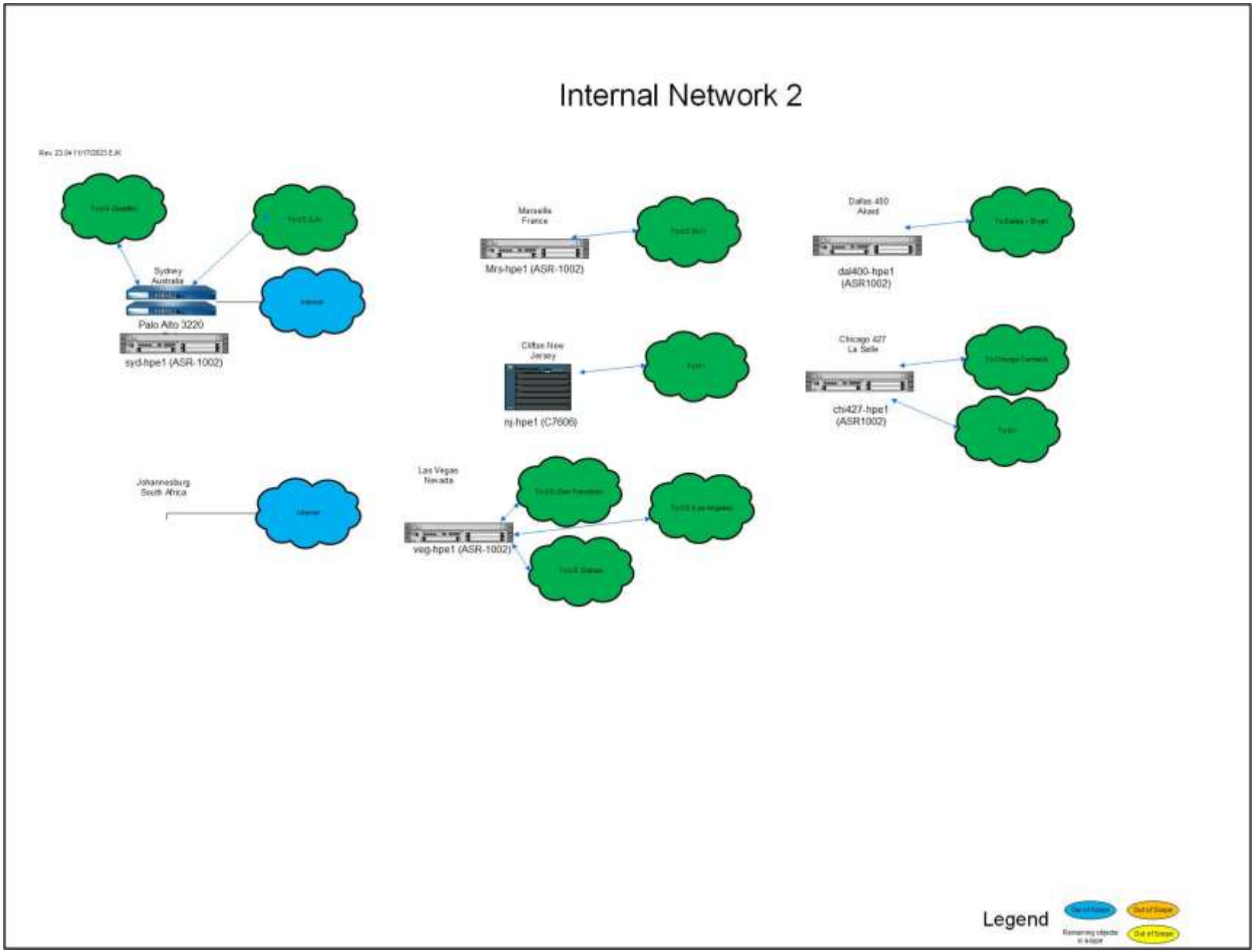
4.1 Detailed network diagram(s)

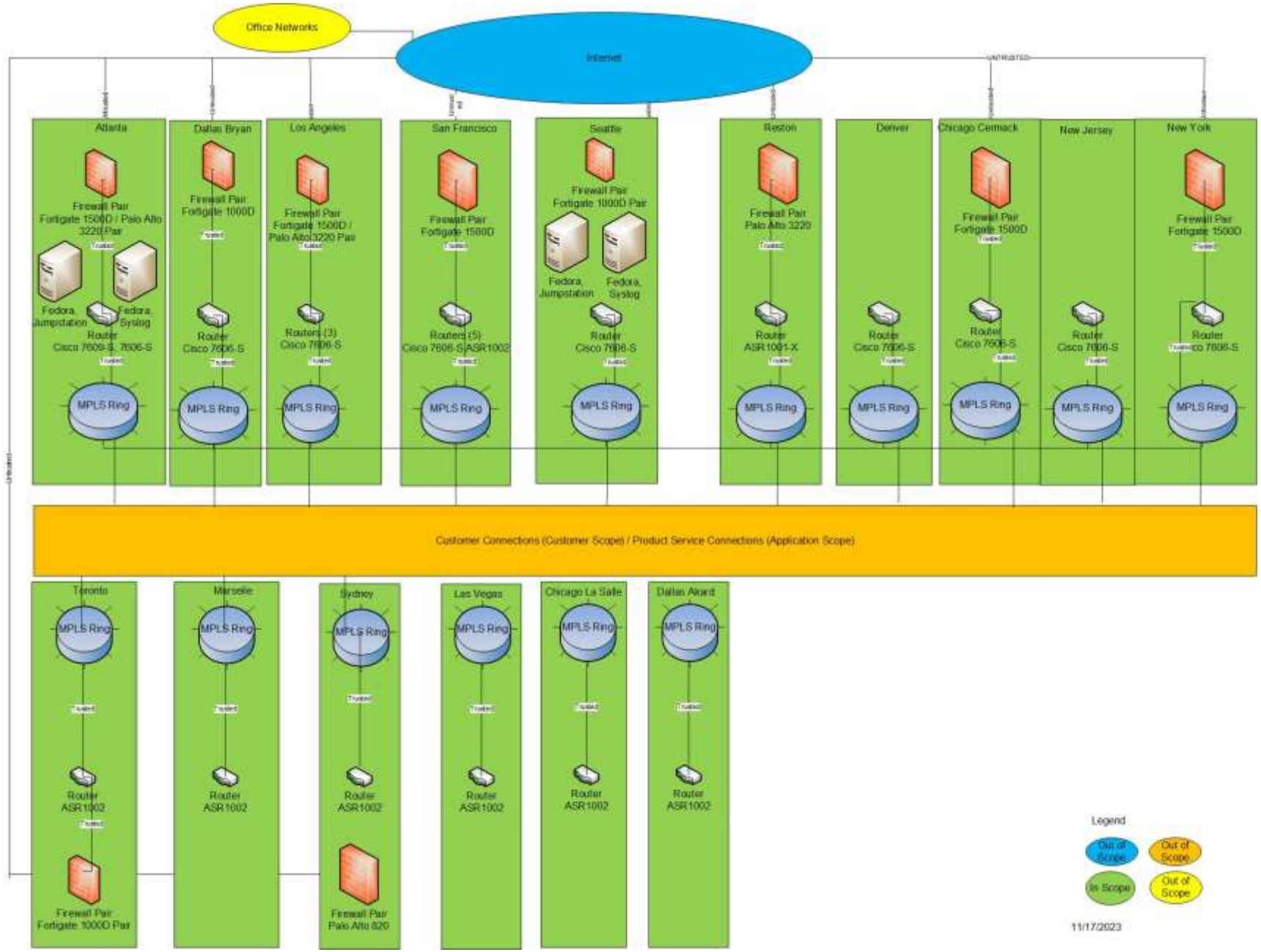
Provide one or more ***detailed diagrams*** to illustrate each communication/connection point between in scope networks/environments/facilities. Diagrams should include the following:

- All boundaries of the cardholder data environment
- Any network segmentation points which are used to reduce scope of the assessment
- Boundaries between trusted and untrusted networks
- Wireless and wired networks
- All other connection points applicable to the assessment

Ensure the diagram(s) include enough detail to clearly understand how each communication point functions and is secured. *(For example, the level of detail may include identifying the types of devices, device interfaces, network technologies, protocols, and security controls applicable to that communication point.)*







4.2 Description of cardholder data flows

Note: *The term "Capture" in Section 4.2 of the ROC Template refers to the specific transaction activity, while the use of "capture" in PCI DSS Requirement 9.9 refers to the receiving of cardholder data via physical contact with a payment card (e.g. via swipe or dip).*

Cardholder data-flow diagrams may also be included as a supplement to the description of how cardholder data is transmitted and/or processed.

Cardholder data flows	Types of CHD involved (for example, full track, PAN, expiry, etc.)	Describe how cardholder data is transmitted and/or processed and for what purpose it is used (for example, which protocols or technologies were used in each transmission)
Capture	Not Applicable	Not Applicable. Sangoma does not capture cardholder data as part of its business model, according to Int-1.
Authorization	Not Applicable	Not Applicable. Sangoma does not authorize cardholder data as part of its business model, according to Int-1.
Settlement	Not Applicable	Not Applicable. Sangoma does not provide settlement, according to Int-1.
Chargeback	Not Applicable	Not Applicable. Sangoma does not provide chargeback services, according to Int-1.
Identify all other data flows, as applicable (add rows as needed)		
Other (describe)	Not Applicable	Not Applicable
Other details regarding the flow of CHD, if applicable:		Not Applicable

4.3 Cardholder data storage

Identify and list all databases, tables, and files storing post-authorization cardholder data and provide the following details.

Note: *The list of files and tables that store cardholder data in the table below must be supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers.*

Data Store (database, etc.)	**File(s) and/or Table(s)**	**Cardholder data elements stored** (for example, PAN, expiry, Name, any elements of SAD, etc.)	**How data is secured** (for example, what type of encryption and strength, hashing algorithm and strength, tokenization, access controls, truncation, etc.)	**How access to data stores is logged** (description of logging mechanism used for logging access to data—for example, describe the enterprise log management solution, application-level logging, operating system logging, etc. in place)
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

4.4 Critical hardware and software in use in the cardholder data environment

Identify and list all types of hardware and critical software in the cardholder environment. Critical hardware includes network components, servers and other mainframes, devices performing security functions, end-user devices (such as laptops and workstations), virtualized devices (if applicable)

and any other critical hardware – including homegrown components. Critical software includes e-commerce applications, applications accessing CHD for non-payment functions (fraud modeling, credit verification, etc.), software performing security functions or enforcing PCI DSS controls, underlying operating systems that store, process or transmit CHD, system management software, virtualization management software, and other critical software – including homegrown software/applications. For each item in the list, provide details for the hardware and software as indicated below. Add rows, as needed.

Critical Hardware			Critical Software		Role/Functionality
Type of Device (for example, firewall, server, IDS, etc.)	**Vendor**	**Make/Model**	**Name of Software Product**	**Version or Release**	
Firewall	FortiNet	FortiGate 1000D	--	--	Customer Firewall
Firewall	FortiNet	FortiGate 1500D	--	--	Customer Firewall
Firewall	Palo Alto	PA-3220	--	--	Application Firewall
Router	Cisco	7606-S	--	--	Edge Router
Router	Cisco	7609-S	--	--	Edge Router
Router	Cisco	7606	--	--	Edge Router
Router	Cisco	ASR1002	--	--	Edge Router
Router	Cisco	ASR1001x	--	--	Edge Router
Switch	Juniper	QFX 5100	--	--	Core Network
Blade Server	Cisco	B200-M4	--	--	Jump Stations, Log Servers
Laptop	Dell	Latitude 5420	--	--	Administrator Workstation/Laptop
Laptop	Apple	MacBook Pro	--	--	Administrator Workstation/Laptop
Workstation	Dell	Optiplex 755	--	--	Administrative Workstation
--	--	--	Fedora	Fedora Core 37	Authentication, Centralized Logging, Name Server, Jump Server
--	--	--	Rsyslog	8.2204.0-3.fc37	Centralized Logging
--	--	--	BIND	9.18.12-1.fc37	Internal DNS (Domain Naming Services)
--	--	--	OpenSSH	8.8p1-7.fc37	Remote Access
--	--	--	OSSEC	v3.3.0	HIDS / change-detection / FIM
--	--	--	Logwatch	7.8-1.fc37	Log Monitoring

Critical Hardware			Critical Software		Role/Functionality
Type of Device (for example, firewall, server, IDS, etc.)	**Vendor**	**Make/Model**	**Name of Software Product**	**Version or Release**	
--	--	--	Microsoft	Windows 10 Home	Administrator Laptop/Workstation
--	--	--	Apple	MacOS 12.6.3	Administrator Laptop/Workstation
--	--	--	Apple	MacOS 12.6.4	Administrator Laptop/Workstation
--	--	--	FortiClient	Endpoint Management Server (EMS) 6.4.8.1755	Antivirus / Anti-Malware
--	--	--	ClamAV	0.101.5-1	Antivirus
--	--	--	FortiGate FortiClient VPN	5.4.1.0840	VPN
--	--	--	Google authenticator plug-in	1.09-5.fc37	Multi-factor Authentication
--	--	--	Tenable Nessus	10.1.1	Internal Scan
--	--	--	Cisco TACACS	TACACS+ F4.0.4.28	Authentication
--	--	--	VMware	4.5.0	SD-Wan management
--	--	--	FortiNet	VDOM	Virtualization (Virtual DOMain)
--	--	--	Nagios	4.4.9-2.fc37	Monitoring Software

4.5 Sampling

Identify whether sampling was used during the assessment.

▪ If sampling is not used:	
– Provide the name of the assessor who attests that every system component and all business facilities have been assessed.	Not Applicable
▪ If sampling is used:	
– Provide the name of the assessor who attests that all sample sets used for this assessment are represented in the below “Sample sets	David M Dennis

for reporting" table. *Examples may include, but are not limited to firewalls, application servers, retail locations, data centers, User IDs, people, etc.*	
– Describe the sampling rationale used for selecting sample sizes (for people, processes, technologies, devices, locations/sites, etc.).	Sampling was selected by the following rationale: For asset pools of under ten, all units were sampled (no sampling used) except for FortiGate, where it was decided that 2 of 10 was a representative sample due to consistent rules set and ACL definitions found. Palo Alto firewalls were sampled at a rate of 2 out of 6 due to consistent rules set and ACL definitions found. Cisco ASR 1002 routers were sampled at 4 out of 8, due to consistency of definitions found. Sample Set-4 was sampled to a unique count due to some unique elements of the builds involved. There were 2 classes of servers, they were sampled at 2 apiece. Sample Set-17 was sampled at 10% of the log file entries, due to the consistent manner in which Sangoma is recording and storing logfiles. For employees, due to the small numbers of total people of a particular job description, at least 50% were sampled. For routers, given their importance, 4 of 12 Cisco 7606-S rules sets were reviewed. The Sangoma build process gave a significant confidence factor that all servers were built and configured using the same process, and as a result I determined that it was not necessary to sample beyond the listed sets.
– If standardized PCI DSS security and operational processes/controls were used for selecting sample sizes, describe how they were validated by the assessor.	I read configurations of servers exported during the assessment process, and compared them to the documented build process. I interviewed knowledgeable individuals, read server and network device configuration, and observed live server processes during Zoom live session.

4.6 Sample sets for reporting

Note: *If sampling is used, this section MUST be completed. When a reporting instruction asks to identify a sample, the QSA may either refer to the Sample Set Reference Number (for example "Sample Set-1") OR list the sampled items individually in the response. Examples of sample sets may include, but are not limited to, firewalls, application servers, retail locations, data centers, User IDs, people, etc. Add rows as needed.*

Sample Set Reference Number	**Sample Type/ Description** (e.g., firewalls, datacenters, change records, User IDs, etc.)	**Listing of all items (devices, locations, change records, people, etc.) in the Sample Set**	**Make/Model of Hardware Components or Version/Release of Software Components**	**Total Sampled**	**Total Population**
Sample Set-1	Firewall	FortiNet	FortiGate 1500D	2	10
		Palo Alto	PA-3220	2	6
Sample Set-2	Router	Cisco	7606-S	4	12

Sample Set Reference Number	Sample Type/ Description (e.g., firewalls, datacenters, change records, User IDs, etc.)	Listing of all items (devices, locations, change records, people, etc.) in the Sample Set	Make/Model of Hardware Components or Version/Release of Software Components	Total Sampled	Total Population
		Cisco	ASR1001x	1	1
		Cisco	7606	4	12
		Cisco	ASR1002	4	8
Sample Set-3	Previous Logged Incidents	Failed login incident	N/A	1	1
		Change	N/A	1	1
Sample Set-4	All Servers	Fedora Core 37	N/A	4	19
Sample Set-5	Authentication Server	TACACS+ Authentication	F4.0.4.28	2	2
Sample Set-6	Logging Server	Rsyslog	8.2204.0-3.fc37	2	2
		Logwatch	7.8-1.fc37	2	2
Sample Set-7	Name Server	BIND	9.18.12-1.fc37	2	2
Sample Set-8	Jump Station	OpenSSH	8.8p1-7.fc37	2	2
Sample Set-9	Operating System Software - Workstations	Mac OS X	12.6.3	1	1
		Mac OS X	12.6.4	1	1
		Microsoft	Windows 10 Home	1	1
Sample Set-10	Firewall Changes	Atl Firewall Update Change Ticket (Doc-54)	N/A	1	1
		Chi Firewall Update Change Ticket (Doc-55)	N/A	1	1
		Dal Firewall Update Change Ticket (Doc-56)	N/A	1	1
Sample Set-11	Router Changes	SDWan Upgrade	N/A	1	1
		FortiGate Upgrade (multiple sites)	N/A	1	1
Sample Set-12	Sample alerts	BGP-3-NOTIFICATION alert	N/A	1	1
		Syslog cannot connect to Postgres	N/A	1	1
Sample Set-13	Patching	FortiNet FortiGate Recommended Patches, Feb 2023 and Change Ticket	N/A	1	1

Sample Set Reference Number	Sample Type/ Description (e.g., firewalls, datacenters, change records, User IDs, etc.)	Listing of all items (devices, locations, change records, people, etc.) in the Sample Set	Make/Model of Hardware Components or Version/Release of Software Components	Total Sampled	Total Population
		Fedora patch list, January 2023	N/A	1	1
Sample Set-14	Senior Engineering User	Int-1, Int-2, Int-3	N/A	3	6
Sample Set-15	Customer Support User	Int-4, Int-7, Int-9	N/A	3	5
Sample Set-16	Co-located Data Centers with AoC	Digital Realty – Atlanta, GA, USA	N/A	18	18
		Digital Realty – Clifton, NJ, USA	N/A		
		Digital Realty – Dallas, TX, USA	N/A		
		Switch – Las Vegas, NV, USA	N/A		
		CoreSite – Los Angeles, CA, USA	N/A		
		Digital Realty – San Francisco, CA, USA	N/A		
		CoreSite – Atlanta, GA, USA	N/A		
		CoreSite – Chicago, IL, USA	N/A		
		Crown Castle (CoreSite) – Los Angeles, CA, USA	N/A		
		CoreSite – Denver, CO, USA	N/A		
		Equinix – Chicago, IL, USA	N/A		
		Equinix – Toronto, ON, Canada	N/A		
		Digital Realty – New York, NY, USA	N/A		
		CoreSite – Reston, VA, USA	N/A		
		Equinix – Sydney, NSW, Australia	N/A		
		Digital Realty – Marseilles, France	N/A		
		Digital Realty– Johannesburg, South Africa	N/A		
Sample Set-17	Sampled log output; centralized log directory. Lognames: 10.64.0.2; 10.64.0.3;	Syslog log enabled	N/A	4	40
		Syslog.log time.set (logfile file names:: 10.64.0.2; 10.64.0.3; 207.232.81.147; 207.232.82.142)	N/A	4	40

Sample Set Reference Number	Sample Type/ Description (e.g., firewalls, datacenters, change records, User IDs, etc.)	Listing of all items (devices, locations, change records, people, etc.) in the Sample Set	Make/Model of Hardware Components or Version/Release of Software Components	Total Sampled	Total Population
	207.232.81.147; 207.232.82.142	Syslog.log access denied (logfile file names:: 10.64.0.2; 10.64.0.3; 207.232.81.147; 207.232.82.142)	N/A	4	40
		Syslog.log administrative actions (logfile file names:: 10.64.0.2; 10.64.0.3; 207.232.81.147; 207.232.82.142)	N/A	4	40
		Syslog.log logging access (logfile file names:: 10.64.0.2; 10.64.0.3; 207.232.81.147; 207.232.82.142)	N/A	4	40
		Syslog.log log file starting audit (logfile file names:: 10.64.0.2; 10.64.0.3; 207.232.81.147; 207.232.82.142)	N/A	4	40
		Syslog.log logging (logfile file names:: 10.64.0.2; 10.64.0.3; 207.232.81.147; 207.232.82.142)	N/A	4	40
Sample Set-18	Co-located Data Centers without AoC	Lunavi – Seattle, WA, USA	N/A	2	2
Sample Set-19	Administrative Laptop Computers	Dell	Latitude 5420	2	2
		Apple MacBook Pro	MacOS 12.6.3	1	1
		Apple MacBook Pro	MacOS 12.6.4	1	1
Sample Set-20	Router Standard Configuration	Doc-11, Doc-12	N/A	2	2
Sample Set-21	Training Records	Doc-26, Doc-27, Doc-28	N/A	3	3

4.7 Service providers and other third parties with which the entity shares cardholder data or that could affect the security of cardholder data

For each service provider or third party, provide:

Note: *These entities are subject to PCI DSS Requirement 12.8.*

Company Name	What data is shared (for example, PAN, expiry date, etc.)	The purpose for sharing the data (for example, third-party storage, transaction processing, etc.)	Status of PCI DSS Compliance (Date of AOC and version #)
Digital Realty	Not Applicable	Collocated hosting	28 Feb 2023; 3.2.1
CoreSite	Not Applicable	Collocated hosting	30 Jun 2023; 3.2.1
Lunavi	Not Applicable	Collocated hosting	Not Applicable
Equinix	Not Applicable	Collocated hosting	5 Nov 2023; 3.2.1

4.8 Third-party payment applications/solutions

Use the table on the following page to identify and list all third-party payment application products and version numbers in use, including whether each payment application has been validated according to PA-DSS or PCI P2PE. Even if a payment application has been PA-DSS or PCI P2PE validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's *PA-DSS Implementation Guide* for PA-DSS applications *or P2PE Implementation Manual (PIM) and* P2PE application vendor's P2PE Application Implementation Guide for PCI P2PE applications/solutions.

Note: *It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.*

Note*: Homegrown payment applications/solutions* ***must*** *be reported at the section for Critical Hardware and Critical Software. It is also strongly suggested to address such homegrown payment applications/solutions below at "Any additional comments or findings" in order to represent all payment applications in the assessed environment in this table.*

Name of Third-Party Payment Application/Solution	Version of Product	PA-DSS validated? (yes/no)	P2PE validated? (yes/no)	PCI SSC listing reference number	Expiry date of listing, if applicable
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
▪ Provide the name of the assessor who attests that all PA-DSS validated payment applications were reviewed to verify they have been implemented in a PCI DSS compliant manner according to the payment application vendor's PA-DSS Implementation Guide				Not Applicable	
▪ Provide the name of the assessor who attests that all PCI SSC-validated P2PE applications and solutions were reviewed to verify they have been implemented in a PCI DSS compliant manner according to the P2PE application vendor's *P2PE Application Implementation Guide* and the P2PE solution vendor's *P2PE Instruction Manual (PIM).*				Not Applicable	
▪ For any of the above Third-Party Payment Applications and/or solutions that are not listed on the PCI SSC website, identify any being considered for scope reduction/exclusion/etc.				Not Applicable	
▪ Any additional comments or findings the assessor would like to include, as applicable:				Not Applicable.	

4.9 Documentation reviewed

Identify and list all reviewed documents. Include the following:

Reference Number *(optional)*	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version date)
Doc-1	SNG CSP 001 Cybersecurity Policy.pdf	The purpose of this policy is to establish the Company requirements to guide personnel behavior on securely managing and handling company data, assets, and IS systems and data.	8 Nov 2023
Doc-2	SNG PR IP 008 Information Protection Policy.pdf	Security policies, processes, and procedures shall be maintained and used to manage protection of information systems and assets.	8 Nov 2023
Doc-3	SNG PR DS 007 Data Security Policy.pdf	The “Company” shall protect the Confidentiality, Integrity, and Availability of all its data at rest, data in transit and data in use within systems in the network.	8 Nov 2023
Doc-4	SNG ID AM 002 Asset Management Policy.pdf	The purpose of this policy is to establish requirements to ensure protection of the "Company's” assets that are accessible by employees and contractors, including mobile assets.	30 Nov 2023
Doc-5	SNG ID BE 003 Business Environment Policy.pdf	The purpose of this policy is to establish requirements to ensure protection of "Company's” supply chain that is accessible by employees and suppliers.	30 Nov 2022
Doc-6	SNG FW PO 018 Firewall Policy.pdf	The purpose of this policy is to secure and protect the information assets owned by The Company. The Company provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives.	13 Oct 2023
Doc-7	SNG PR AC 005 Access Control Policy.pdf	The purpose of this policy is to establish requirements to ensure proper access to The "Company's” information that is accessible by employees and contractors.	8 Nov 2023
Doc-8	NF GUI LINUX Linux Server Guidelines.docx	Linux Server Guidelines	20 May 2022
Doc-9	Equinix Global PCI SOC 2023.pdf	Equinix AOC; v3.2.1	5 Nov 2023
Doc-10	Router Security Guidlines.docx	This document describes a required minimal security configuration for all routers and switches connecting to	17 Jan 2022

		a production network or used in a production capacity at or on behalf of The Company.	
Doc-11	cisco router config diffs1.msg	Router MPLS standard template configuration	19 Feb 2024
Doc-12	cisco router config diffs2.msg	Router non-MPLS standard template configuration	19 Feb 2024
Doc-13	Server Security Guidline.docx	The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by The Company.	17 Jan 2022
Doc-14	InventoryPCIscope.xlsx	Inclusive PCI inventory, including Site Locations and Service Providers, Hardware and Software Inventory, and Appliances.	19 Jan 2024
Doc-15	FortiClient_EMS_7.2.3_Administration_Guide.pdf	FortiGate administrators' installation and maintenance guide	20 Oct 20023
Doc-16	SNG LO AU 019 Audit and Logging Policy.pdf	The purpose of this policy is to secure and protect the information assets owned by The Company. The Company provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives.	8 Nov 2023
Doc-17	SNG IR PO 015 Incident Reporting Policy.pdf	Incident Response Policy	8 Nov 2023
Doc-18	Risk Summary CYQ1-2023.xlsx	Risk Tracker	21 Mar 2023
Doc-19	SNG ID RM 004 Risk Management Policy.pdf	Risk Management, Vulnerability Management. The purpose of this policy is to establish requirements to ensure management of risk within "the Company's" technology that is accessible by employees, contractors and suppliers. Includes quarterly policy review.	8 Nov 2023
Doc-20	SNG WF PO 017 Wireless Communications Policy.pdf	This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to The Company network.	8 Nov 2023
Doc-21	Cisco Router Configuration Guidelines.docx	Cisco Router Operational Guide – access, patching, configuration, access-lists, hardening, logging.	17 Jan 2022
Doc-22	PCI August 2023.pdf	CoreSite AOC, v3.2.1	30 Jun 2023
Doc-23	SNG BCP 020 Business Continuity Policy.pdf	Business Continuity Plan	3 Apr 2023
Doc-24	tw-hardening-junos-devices-checklist.pdf	Juniper Recommended	19 Feb 2024
Doc-25	Firewall_Configuration_Standard_Template.txt	Sangoma standard firewall FortiGate configuration	22 Jan 2024
Doc-26	knowbe4-eric.png	Security Training Portal Snapshot	19 Feb 2024

Doc-27	knowbe4-Jeremy.png	Security Training Portal Snapshot	19 Feb 2024
Doc-28	knowbe4-Liz.png	Security Training Portal Snapshot	19 Feb 2024
Doc-29	Standard External Network Penetration Test_03162023204227.pdf	External Penetration Test	16 Mar 2023
Doc-30	Responsibility Matrix.xlsx	List of PCI Requirements provided by Sangoma	19 Feb 2024
Doc-31	External_Scan_3513173_20230522_120516.pdf	ASV Scan	22 May 2023
Doc-32	External_Scan_3513173_20230822_120519.pdf	ASV Scan	22 Aug 2023
Doc-33	External_Scan_3513173_20231114_150455.pdf	ASV Scan	14 Nov 2023
Doc-34	External_Scan_3513173_20240113_160557.pdf	ASV Scan	13 Jan 2024
Doc-35	Full report - Standard External Network Penetration Test - 02122024141955.pdf	External Pen Test	7 Feb 2024
Doc-36	Full report - Standard Internal Network Penetration Test - 02132024092932.pdf	Internal Pen Test	7 Feb 2024
Doc-37	Internal PCI West_4tjioh.csv	Internal Scan	20 May 2023
Doc-38	Internal PCI West_cl531c.csv	Internal Scan	19 Aug 2023
Doc-39	Internal PCI West_ivcbhl.csv	Internal Scan	21 Nov 2023
Doc-40	Internal PCI West_ysm4t0.csv	Internal Scan	20 Feb 2024
Doc-41	New Connection Procedures.docx	Internal Sangoma turn-up procedures.	17 Mar 2023
Doc-42	Diagram1.jpg	High Level Diagram	17 Nov 2023
Doc-43	Diagram2.jpg	High Level Diagram	17 Nov 2023
Doc-44	Segmentation.jpg	Detailed Diagram showing Segmentation	17 Nov 2023
Doc-45	Digital Realty - 2023 PCI DSS v3.21 - AOCv3.pdf	Digital Realty AOC, v3.2.1	28 Feb 2023
Doc-46	termination update.docx	Terminated User Confirmation	5 Mar 2024
Doc-47	User Management Procedures_Tacacs.docx	Administrative login procedures	22 Jan 2024
Doc-48	ClamAV Documentation.pdf	ClamAV Administrator Guide	22 Jan 2024
Doc-49	Internal PCI East_9fjpk6.csv	Internal Scan	15 May 2023
Doc-50	Internal PCI East_akr1zw.csv	Internal Scan	14 Aug 2023
Doc-51	Internal PCI East_if2ruk.csv	Internal Scan	15 Nov 2023
Doc-52	Internal PCI East_nvfred.csv	Internal Scan	15 Feb 2024
Doc-53	SNG RS RP 012 Incident Response Policy.pdf	The purpose of this policy is to establish requirements to ensure protection of "Company's" information	3 Apr 2023

		that is accessible by employees.	
Doc-54	Change Control form atl-fg2_upgrade.docx	Atl Firewall Change	19 Feb 2024
Doc-55	Change Control form chi-fg2_upgrade.docx	Chi Firewall Change	19 Feb 2024
Doc-56	Change Control form dal-fg1_upgrade.docx	Dal Firewall Change	19 Feb 2024
Doc-57	External_Scan_3513173_20240321_0838.pdf	ASV Scan	21 Mar 2024

4.10 Individuals interviewed

Identify and list the individuals interviewed. Include the following:

Reference Number *(optional)*	Employee Name	Role/Job Title	Organization	Is this person an ISA? (yes/no)
Int-1	Eric Krichbaum	Information Security Officer	Sangoma	No
Int-2	David Lee	VP Engineering	Sangoma	No
Int-3	Toshi Esumi	Network Engineering Manager	Sangoma	No
Int-4	Brian Beam	NOC Technician	Sangoma	No
Int-5	Liz Casale	Network Engineer	Sangoma	No
Int-6	Harrison Pak	Sr. Manager of Cloud Operations	Sangoma	No
Int-7	Warren Romero	Implementation NOC	Sangoma	No
Int-8	Katie Rummell	Senior Director People and Talent	Sangoma	No
Int-9	Brian Wilson	CPE Engineer	Sangoma	No
Int-10	Jacob Landreth	Technician 1	Lunavi	No

4.11 Managed service providers

For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans:

▪ Identify whether the entity being assessed is a managed service provider. **(yes/no)**	no
▪ *If "yes":*	
– List the requirements that apply to the MSP and are included in this assessment.	Not Applicable

– List the requirements that are the responsibility of the MSP's customers (and have not been included in this assessment).	Not Applicable
– Provide the name of the assessor who attests that the testing of these requirements and/or responsibilities of the MSP is accurately represented in the signed Attestation of Compliance.	Not Applicable
– Identify which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans.	Not Applicable
– Identify which of the MSP's IP addresses are the responsibility of the MSP's customers.	Not Applicable

4.12 Disclosure summary for "In Place with Compensating Control" responses

▪ Identify whether there were any responses indicated as "In Place with Compensating Control." **(yes/no)**	no
▪ *If "yes," complete the table below:*	

List of all requirements/testing procedures with this result	**Summary of the issue** (legal obligation, etc.)
Not Applicable	Not Applicable

4.13 Disclosure summary for "Not Tested" responses

▪ Identify whether there were any responses indicated as "Not Tested": **(yes/no)**	no
▪ *If "yes," complete the table below:*	

List of all requirements/testing procedures with this result	**Summary of the issue** (for example, not deemed in scope for the assessment, etc.)
Not Applicable	Not Applicable

5. Quarterly Scan Results

5.1 Quarterly scan results

▪ Is this the assessed entity's initial PCI DSS compliance validation? **(yes/no)**	no

▪ Identify how many external quarterly ASV scans were performed within the last 12 months:	Four (4)

▪ *Summarize* the four most recent quarterly ASV scan results in the Summary Overview as well as in comments at Requirement 11.2.2.

Note: *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verified:*

- *The most recent scan result was a passing scan,*
- *The entity has documented policies and procedures requiring quarterly scanning going forward, and*
- *Any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan.*

For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.

▪ For each quarterly ASV scan performed within the last 12 months, identify:

Date of the scan(s)	Name of ASV that performed the scan	Were any vulnerabilities found that resulted in a failed initial scan? (yes/no)	For all scans resulting in a Fail, provide date(s) of re-scans showing that the vulnerabilities have been corrected
22 May 2023	VikingCloud	No	Not Applicable
22 Aug 2023	VikingCloud	Yes	14 Nov 2023
14 Nov 2023	VikingCloud	No	Not Applicable
13 Jan 2024	VikingCloud	Yes	21 Mar 2024
21 Mar 2024	VikingCloud	No	Not Applicable

If this is the initial PCI DSS compliance validation*, complete the following:*	
▪ Provide the name of the assessor who attests that the most recent scan result was verified to be a passing scan.	Not Applicable
▪ Identify the name of the document the assessor verified to include the entity's documented policies and procedures requiring quarterly scanning going forward.	Not Applicable
▪ Describe how the assessor verified that any vulnerabilities noted in the initial scan have been corrected, as shown in a re-scan.	Not Applicable

Date of the scan(s)	Name of ASV that performed the scan	Were any vulnerabilities found that resulted in a failed initial scan? (yes/no)	For all scans resulting in a Fail, provide date(s) of re-scans showing that the vulnerabilities have been corrected
Assessor comments, if applicable:			An upstream configuration issue was causing ASV scan fails to occur which were related to a patching issue in the network. These were performed until Q1 2024. Sangoma performed regular ASV scans with follow-up to confirm patching at their end was not involved during every quarter as required by PCI-DSS 3.2.1.

5.2 Attestations of scan compliance

Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI DSS Approved Scanning Vendors (ASV) Program Guide.*

Provide the name of the assessor who attests that the ASV and the entity have completed the Attestations of Scan Compliance confirming that all externally accessible (Internet-facing) IP addresses in existence at the entity were appropriately scoped for the ASV scans:	David M Dennis

6. Findings and Observations

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.			☒	☐	☐	☐	☐
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections, and • Changes to firewall and router configurations.	**Identify the document(s)** reviewed to verify procedures define the formal processes for:						
	• Testing and approval of all network connections.	*Doc-4* *Doc-6* *Doc-10*					
	• Testing and approval of all changes to firewall and router configurations.	*Doc-4* *Doc-6* *Doc-10*					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	**Identify the sample of records** for network connections that were selected for this testing procedure.	*Sample Set-10* *Sample Set-11*					
	Identify the responsible personnel interviewed who confirm that network connections were approved and tested.	*Int-3* *Int-4* *Int-9*					
	Describe how the sampled records verified that network connections were:						
	• Approved	*I reviewed Sample Set-10 VDOM definitions for customer connectivity to office; and Sample Set-11 router ACL for external-facing IP and routing protocol during live Zoom review, and observed that the tracking tickets for network revisions for customers' connections had an approval required tab on each change sampled. I observed that these tracker tabs had an approver who signed off on the changes.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Tested	*I compared the changes in Sample Set-10 and Sample Set-11 to the procedure in Doc-6 and found that the new IP addresses were tested/pinged by "turn-up" team member who commented in the ticket. I found testing was confirmed by Int-1 as having been approved, Approval was given once testing had been performed.*					
1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	**Identify the sample of records** for firewall and router configuration changes that were selected for this testing procedure.	*Sample Set-10* *Sample Set-11*					
	Identify the responsible personnel interviewed who confirm that changes made to firewall and router configurations were approved and tested.	*Int-1* *Int-4* *Int-9*					
	Describe how the sampled records verified that the firewall and router configuration changes were:						
	• Approved	*I requested and obtained a sample of tickets showing changes to the network connections. I observed during live Zoom session of Sample Set-10 VDOM change for office addition and Sample Set-11 for external-facing IP and these tickets showed changes to the network connections which enabled a new payment processor connection, and which took out support for an obsolete one. I observed Sample Set-1 and Sample Set-2 for the same change, and found it was commented with the same ticket number. The tickets showed that the changes had to be approved, and there was also a box that had to be signed for testing. Finally the ticket had a sign-off by compliance - management approval by Int-1 authorizing the change or install. These items led to a determination of compliance.*					
	• Tested	*Int-1 pointed out the procedure they follow, which required that the changes be tested, and testing to be approved by the requestor on the ticket. If requestor on ticket signs off, the change test was approved. Approval sign-off was seen on tickets in Sample Set-10 and Sample Set-11.*					
1.1.2 Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.			☒	☐	☐	☐	☐
	Identify the current network diagram(s) examined.	*Doc-42*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to the cardholder data environment, including any wireless networks.	**Describe how** network configurations verified that the diagram:						
	• Is current.	*I reviewed Sample Set-1 and Sample Set-2 with Int-1 during live Zoom remote site visit. I asked to see VLAN definitions as described on the diagrams. I asked to see changes documented that matched Sample Set-10 and Sample Set-11. I observed that the diagram date was after all changes. I found no network detail (VLAN or ACL connection) in the configuration that did not match the diagrams. I observed by these reviews that the diagrams were current and kept up to date.*					
	• Includes all connections to cardholder data.	*I observed firewall rules comments with network names and city locations in the firewall rules in Sample Set-1 with Int-1 assistance, and observed that these connections matched the network diagram Doc-42, Doc-43, and Doc-44 for every node on the Sangoma network identified as being in-scope.*					
	• Includes any wireless network connections.	*Not Applicable. I observed by review of Doc-42, Doc-43 and Doc-44 that there are no wi-fi networks in use at Sangoma.*					
1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	**Identify the responsible personnel** interviewed who confirm that the diagram is kept current.	*Int-1*					
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.			☐	☐	☒	☐	☐
1.1.3.a Examine data flow diagram and interview personnel to verify the diagram: • Shows all cardholder data flows across systems and networks. • Is kept current and updated as needed upon changes to the environment.	**Identify the data-flow diagram**(s) examined.	*Not Applicable. I observed by interview with Int-1 and review of Doc-42, Doc-43, and Doc-44 that Sangoma has no data flow on its network.*					
	Identify the responsible personnel interviewed who confirm that the diagram: • Shows all cardholder data flows across systems and networks. • Is kept current and updated as needed upon changes to the environment.	*Not Applicable*					
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1.4.a Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	**Identify the firewall configuration standards document** examined to verify requirements for a firewall: • At each Internet connection. • Between any DMZ and the internal network zone.	*Doc-6* *Doc-25*					
1.1.4.b Verify that the current network diagram is consistent with the firewall configuration standards.	**Provide the name of the assessor** who attests that the current network diagram is consistent with the firewall configuration standards.	*David M Dennis*					
1.1.4.c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams.	**Describe how** network configurations verified that, per the documented configuration standards and network diagrams, a firewall is in place:						
	• At each Internet connection.	*I interviewed Int-1 during live Zoom session, and reviewed Sample Set-1 and Sample Set-2 and found the following: The border router and the FortiGate are configured so that all connections are required to be through the FortiGate. The segmentation is on the back end. Customer connections to the routing infrastructure must traverse the Fortinet FortiGate 1000D and Fortinet FortiGate 1500D to reach the internet segment. No connection exists between customer routers and internet, by firewall policy. I observed that the customer is inside a VRF (Virtual Routing and Forwarding) which is defined in router policy. Observed by vrf def route designator and confirmed that they are unique to customer. I observed that Route Designator and Route Target, which maps to customer interface and maps to the name of the VRF, were used in Sample Set-1, as described by Doc-6 and Doc-25. By reviewing these details with Int-1, I was able to determine that a firewall is in place at each Sangoma connection.*					
	• Between any DMZ and the internal network zone.	*I examined the Sample Set-2 configurations during live Zoom session for Atl-hpe1, Ny-hpe1, Chi-hpe1, Den-hpe1, Sea-hpe1, Sjc-hpe1, sfo-core1, sfo-core2, La-hpe1, La-hpe2 and Dal-hpe1 and found that Sangoma has rules that cover the IP ranges for their DMZ and their internal administrative and support VLANs. This matched what is shown by Doc-43.*					
1.1.5 Description of groups, roles, and responsibilities for management of network components.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1.5.a Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.	**Identify the firewall and router configuration standards document(s)** reviewed to verify they include a description of groups, roles and responsibilities for management of network components.	*Doc-6* *Doc-10*					
1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.	**Identify the responsible personnel** interviewed who confirm that roles and responsibilities are assigned as documented.	*Int-1*					
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.			☒	☐	☐	☐	☐
1.1.6.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each.	**Identify the firewall and router configuration standards document(s)** reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification and approval for each.	*Doc-6* *Doc-10*					
1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.	**Indicate whether** any insecure services, protocols or ports are allowed. **(yes/no)**	*no*					
	If "yes," complete the instructions below for EACH insecure service, protocol, and port allowed: (add rows as needed)						
	Identify the firewall and router configuration standards document(s) reviewed to verify that security features are documented for each insecure service/protocol/port.	*Not Applicable*					
1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.	*If "yes" at 1.1.6.b, complete the following for each insecure service, protocol, and/or port present (add rows as needed):*						
	Describe how firewall and router configurations verified that the documented security features are implemented for each insecure service, protocol and/or port.	*Not Applicable. No insecure services are allowed by Sangoma configuration.*					
1.1.7 Requirement to review firewall and router rule sets at least every six months.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1.7.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	**Identify the firewall and router configuration standards document(s)** reviewed to verify they require a review of firewall rule sets at least every six months.	*Doc-1* *Doc-6*					
1.1.7.b Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.	**Identify the document(s) relating to rule set reviews** that were examined to verify that rule sets are reviewed at least every six months for firewall and router rule sets.	*Doc-16*					
	Identify the responsible personnel interviewed who confirm that rule sets are reviewed at least every six months for firewall and router rule sets.	*Int-1*					
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*							
1.2 Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment:							
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.			☒	☐	☐	☐	☐
1.2.1.a Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.	**Identify the firewall and router configuration standards document(s)** reviewed to verify they identify inbound and outbound traffic necessary for the cardholder data environment.	*Not Applicable. I reviewed Doc-42 and Doc-43 and interviewed Int-1 and Int-2 to confirm that there is no cardholder data environment managed by Sangoma.*					
1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.	**Describe how** firewall and router configurations verified that the following traffic is limited to that which is necessary for the cardholder data environment:						
	• Inbound traffic	*Not Applicable. I reviewed Doc-42, Doc-43 and Doc-44 and interviewed Int-1 and Int-2 to confirm there is no cardholder data environment managed by Sangoma, and this includes inbound traffic to a CHD environment.*					
	• Outbound traffic	*Not Applicable. I reviewed Doc-42, Doc-43 and Doc-44 and interviewed Int-1 and Int-2 to confirm that there is no cardholder data environment managed by Sangoma, and this includes outbound traffic from a CHD environment.*					
	Describe how firewall and router configurations verified that the following is specifically denied:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	• All other inbound traffic	*I reviewed the firewall configuration for Sample Set-1 and found that there was an explicit deny-all ingress object defined. Int-1 explained this rule was used when traffic did not match allowed rules.* *I reviewed in Sample Set-2 that public-facing requirements for routed data inbound from public included peer network groups between data center routers. This data included SSH traffic permits inbound for jump servers. All other traffic, as well as traffic to the inbound interfaces of the customer environment, were not permitted.*					
	• All other outbound traffic	*I reviewed the firewall configuration for Sample Set-1 and found that there were defined ACL objects to match specific trusted destinations for the network. Int-1 explained these were devices that Sangoma allowed traffic to pass for, and IP ranges that were not specifically allowed would be denied by a default deny-all that existed.* *I reviewed in Sample Set-2 that public-facing requirements for routed data outbound from public included peer network groups between data center routers. This data included SSH traffic permits outbound for jump servers. All other traffic, as well as traffic to the outbound interfaces of the customer environment, were not permitted.*					
1.2.2 Secure and synchronize router configuration files.			☒	☐	☐	☐	☐
1.2.2.a Examine router configuration files to verify they are secured from unauthorized access.	**Describe how** router configuration files are secured from unauthorized access.	*I reviewed Sample Set-5 with assistance from Int-1 and observed that 'wheel' privileged user class. This user class was then located on the approved IP address list provided as part of Doc-6. Finally, this list was in the Sample Set-2 router ACL rules provided. As a result, access to routers is allowed only by approved IP origin by approved authorized privileged individual login.*					
1.2.2.b Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).	**Describe how** router configurations are synchronized.	*I reviewed the boot file provided as part of the router engine rules provided in Sample Set-2. I compared the boot file rules with the show-running rules provided by Int-1 and observed that the rules matched on every data element examined.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.			☐	☐	☒	☐	☐
1.2.3.a Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.	**Describe how** firewall and router configurations verified that perimeter firewalls are in place between all wireless networks and the cardholder data environment.	*Not Applicable. I read Sample Set-1 and Doc 43, Doc-44 and Doc-45 to find that no wi-fi exists in the Sangoma in-scope environment.*					
1.2.3.b Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**Indicate whether** traffic between the wireless environment and the cardholder data environment is necessary for business purposes. **(yes/no)**	*no*					
	If "no":						
	Describe how firewall and/or router configurations verified that firewalls deny all traffic from any wireless environment into the cardholder environment.	*Not Applicable. During live Zoom review with assistance from Int-1 I reviewed Sample Set-1 and Sample Set-2. With assistance from Int-1 I reviewed Sample Set-1 and Sample Set-2 to observe that no IP access permit was in place in the configurations to allow this IP origin any access to the in-scope network, and was told that this office is air-gapped from all in-scope networks. I reviewed Sample Set-1 to determine that no direct access exists; and I observed in Sample Set-5 that to access this network, engineers must use multi-factor VPN. I observed by firewall rules in Sample Set-1 that no CDE data traffic can pass upstream to the wireless network.*					
	If "yes":						
	Describe how firewall and/or router configurations verified that firewalls permit only authorized traffic from any wireless environment into the cardholder environment.	*Not Applicable*					
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.							
1.3 Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment:							
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.3.1 Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**Describe how** firewall and router configurations verified that the DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	*With assistance from Int-1 and Int-3, I observed FortiGate VDOM definitions for root and customer VDOM (Virtual Domain). I observed that log groups, management groups and route groups are applied to the VDOM, resulting in no routable path for the DMZ to pass into the in-scope management network on any port. The "allow access" variable was Unset, which disallows customer from affecting the admin (in-scope) network.* *I observed in Sample Set-2 Cisco routers contained a DMZ definition which allowed no inbound connections to occur, other than from trusted network for jump server on a specific IP address.*					
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.			☒	☐	☐	☐	☐
1.3.2 Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.	**Describe how** firewall and router configurations verified that configurations limit inbound Internet traffic to IP addresses within the DMZ.	*With assistance from Int-1 and Int-3 I observed that FortiNet FortiGate 1500D firewall VDOMS are different in the configuration, which I had explained meant that internet inbound traffic cannot reach past the desired target and cannot cross to sensitive admin network. The Root VDOM (admin) of the FortiNet FortiGate 1500D and Customer VDOMs communication are not allowed by default.* *I observed with assistance from Int-1 in Sample Set-2 Cisco routers contained ACL that denied all traffic from untrusted origin. Only administrative traffic (login default group tacacs-mgt group tacacs+ enable) is allowed to pass from outside world to the DMZ, and this traffic is only allowed if MFA / TACACS+ is successfully authorized. I observed the only external IP addresses from the internet that were granted any ability to traverse were definitions for the administrative jump-boxes in the DMZ, and that these also required MFA and TACACS+. This led to a determination of compliance.*					
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. *(For example, block traffic originating from the Internet with an internal source address)*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.3.3 Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ**.**	**Describe how** firewall and router configurations verified that anti-spoofing measures are implemented.	*I asked for and was provided with snapshot rules sets for the Root VDOM and customer VDOM in FortiNet FortiGate 1500D and the defined groups in Palo Alto PA-3220 in Sample Set-1 and Cisco 7606-S. Cisco 7609-S, Cisco 7606, and Cisco ASR 1002 in Sample Set-2. I observed with assistance from Int-1 and Int-3 that the Root VDOM has no permissions to talk to internet by default. In configuration the set IP command is used to set defaults. ICMP redirect is allowed but forwarding IP is not allowed by default. This results in no inbound traffic being able to reach the in-scope network. I asked for assistance from Int-1 and found the configuration in use includes source route validation and statefulness. Int-1 explained that these were anti-spoofing measures.*					
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.			☐	☐	☒	☐	☐
1.3.4 Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	**Describe how** firewall and router configurations verified that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	*Not Applicable. I reviewed Doc-42, Doc-43 and Doc-44 and interviewed Int-1 and Int-2 to observe that there is no cardholder data environment that Sangoma has defined or is responsible for in their network.*					
1.3.5 Permit only "established" connections into the network.			☒	☐	☐	☐	☐
1.3.5 Examine firewall and router configurations to verify that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session.	**Describe how** firewall and router configurations verified that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session	*I asked for and was shown with assistance from Int-1 the VDOM definitions in Sample Set-1. I observed that VDOM root NAT is enabled from customer side. This indicated that stateful inspection was enabled by default, as this feature requires stateful inspection to function.*					
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.			☐	☐	☒	☐	☐
1.3.6 Examine firewall and router configurations to verify that system components that store cardholder data	**Indicate whether** any system components store cardholder data. **(yes/no)**	*no*					
	If "yes":						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
are on an internal network zone, segregated from the DMZ and other untrusted networks.	**Describe how** firewall and router configurations verified that the system components that store cardholder data are located on an internal network zone, and are segregated from the DMZ and other untrusted networks.	*Not Applicable. Sangoma systems do not store cardholder data.*					
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. *Note: Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT),* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*			☒	☐	☐	☐	☐
1.3.7.a Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	**Describe how** firewall and router configurations verified that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	*I reviewed configurations in Sample Set-1 and Sample Set-2 with assistance from Int-1 and Int-3. I observed that NAT is enabled on firewalls and used exclusively for server IP addressing. Public-facing IP are able to reach the gateway firewalls only, and only when appropriately configured for a specific IP address. I read firewall rules in Sample Set-1 and found NAT is enabled on all rules sets. I read that private IP (RFC 1918 and RFC 6890) is disabled from being routed beyond local area network. I read in firewall rules that no private IP has a direct allowed path to any external IP.*					
1.3.7.b Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.	**Identify the document** reviewed that specifies whether any disclosure of private IP addresses and routing information to external parties is permitted.	*Doc-1*					
	For each permitted disclosure, **identify the responsible personnel** interviewed who confirm that the disclosure is authorized.	*Int-1*					
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.4.a Examine policies and configuration standards to verify: • Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. • Specific configuration settings are defined for personal firewall or equivalent functionality. • Personal firewall or equivalent functionality is configured to actively run. • Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices.	**Indicate whether** portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network are used to access the organization's CDE. **(yes/no)**	*yes*					
	If "no," **identify the document** reviewed that explicitly prohibits portable computing devices (including company and/or employee-owned) with direct connectivity to the Internet when outside the network from being used to access the organization's CDE. *Mark 1.4.b as "not applicable"*	*Not Applicable*					
	If "yes," **identify the documented policies and configuration standards** that define the following: • Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE. • Specific configuration settings are defined for personal firewall or equivalent functionality. • Personal firewall or equivalent functionality is configured to actively run. • Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices.	*Doc-2*					
	Identify the sample of mobile and/or employee-owned devices selected for this testing procedure.	*Sample Set-19*					
	Describe how the sample of portable computing devices (including company and/or employee-owned) verified that personal firewall software is:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.4.b Inspect a sample of portable computing devices (including company and/or employee-owned) to verify that: • Personal firewall (or equivalent functionality) is installed and configured per the organization's specific configuration settings. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall or equivalent functionality is not alterable by users of the portable computing devices.	• Installed and configured per the organization's specific configuration settings.	*I observed the operating systems running on Sample Set-19 with assistance from Int-1 via a remote Zoom meeting. I observed that the demonstration workstation matched the required configuration to have Fortigate firewalls always be running on employee workstations, which Int-1 said were "Firewall On" setting, with "Turn Off Firewall" greyed out. All configurations matched, which is as documented required by Doc-4. These findings supported a determination of compliance.*					
	• Actively running.	*I observed that the software client screens in the desktop firewall management screens shown to me during a Zoom meeting to review Sample Set-19. I observed that these clients were running, and all had the "green" indicator shown. The green running indicator indicated that the installed software was operating, and this supported a determination of compliance.*					
	• Not alterable by users of mobile and/or employee-owned devices.	*The software client screens I observed during remote Zoom meeting in Sample Set-19 were all greyed out for "Turn Off Firewall" as observed during the remote Zoom meeting, and matched.*					
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
1.5 Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are: • Documented, • In use, and • Known to all affected parties.	**Identify the document reviewed** to verify that security policies and operational procedures for managing firewalls are documented.	*Doc-1* *Doc-6*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for managing firewalls are: • In use • Known to all affected parties	*Int-1* *Int-2* *Int-4*					

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. *This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.*			☒	☐	☐	☐	☐
2.1.a Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-2* *Sample Set-4*					
	Identify the vendor manuals and sources on the Internet used to find vendor-supplied accounts/passwords.	*Doc-15* *Doc-21* *Doc-24* *https://docs.fedoraproject.org/en-US/fedora/f31/system-administrators-guide/*					
	For each item in the sample, **describe how** attempts to log on to the sample of devices and applications using default vendor-supplied accounts and passwords verified that all default passwords have been changed.	*I observed by remote live Zoom session while Int-5 logged into sampled servers, routers, and firewalls. Known / documented system default logins for Linux and for network devices failed when tried. Routers in Sample Set-2 did not allow default "admin/cisco" to log in with any test tried. Firewalls in Sample Set-1 did not allow Fortinet default of "admin" and (blank) password. Linux servers in Sample Set-4 did not allow root / root, or other well-known defaults to work in any observed sample. Because these defaults did not work, I was able to determine that the default factory reset passwords had been changed, and this led to a determination of compliance. I observed by remote live Zoom session while Int-5 logged into Cisco device, that the default password to access did not work. I observed that Doc-24 guidance was followed.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.1.b For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	*For each item in the sample of system components indicated at 2.1.a, **describe how** all unnecessary default accounts were verified to be **either**:*						
	• Removed	*I observed during Zoom review with assistance from Int-5, that In the case of Sample Set-2, the default "user admin / password cisco" was tried by Int-5, and these failed in every observed instance. In the case of Fortinet in Sample Set-1, I observed while Int-1 attempted to Telnet into the devices, and the Telnet daemon was not responding, so there was no way to use the default account. I interviewed Int-4 who confirmed that default Telnet is removed prior to deployment. I observed in Sample Set-4 that Linux servers did not remove default accounts, but disabled them, so the disabled requirement was more appropriate to address.*					
	• Disabled	*For Linux servers observed in Sample Set-4 with Int-1's assistance during Zoom review, a list of default Linux users was observed to be configured to have "/bin/nologin" in the login shell, which I was told by Int-2 that this disables the shell for users. I asked to see and was shown attempted logins with FTP, daemon, adm accounts, and observed that no login account was given or login session possible.*					
2.1.c Interview personnel and examine supporting documentation to verify that: • All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. • Unnecessary default accounts (including accounts used by operating	**Identify the responsible personnel** interviewed who verify that: • All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc. are changed before a system is installed on the network. • Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	*Int-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	**Identify supporting documentation** examined to verify that: • All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. • Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.	*Doc-2* *Doc-4* *Doc-6* *Doc-13*					
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.			☐	☐	☒	☐	☐
2.1.1.a Interview responsible personnel and examine supporting documentation to verify that: • Encryption keys were changed from default at installation • Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions.	**Indicate whether** there are wireless environments connected to the cardholder data environment or transmitting cardholder data. **(yes/no)** *If "no," mark 2.1.1 as "Not Applicable" and proceed to 2.2.*	*no*					
	If "yes":						
	Identify the responsible personnel interviewed who verify that encryption keys are changed: • From default at installation • Anytime anyone with knowledge of the keys leaves the company or changes positions.	*Not Applicable. Sangoma does not have any wireless environments connected to the in-scope environment.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify supporting documentation examined to verify that: • Encryption keys were changed from default at installation • Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions.	*Not Applicable*					
2.1.1.b Interview personnel and examine policies and procedures to verify: • Default SNMP community strings are required to be changed upon installation. • Default passwords/phrases on access points are required to be changed upon installation.	**Identify the responsible personnel** interviewed who verify that: • Default SNMP community strings are required to be changed upon installation. • Default passwords/passphrases on access points are required to be changed upon installation.	*Not Applicable*					
	Identify policies and procedures examined to verify that: • Default SNMP community strings are required to be changed upon installation. • Default passwords/phrases on access points are required to be changed upon installation.	*Not Applicable*					
2.1.1.c Examine vendor documentation and login to wireless devices, with system administrator help, to verify: • Default SNMP community strings are not used. • Default passwords/passphrases on access points are not used.	**Identify vendor documentation** examined to verify that: • Default SNMP community strings are not used. • Default passwords/passphrases on access points are not used.	*Not Applicable*					
	Describe how attempts to login to wireless devices verified that:						
	• Default SNMP community strings are not used.	*Not Applicable*					
	• Default passwords/passphrases on access points are not used.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.1.1.d Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for: • Authentication over wireless networks • Transmission over wireless networks	**Identify vendor documentation** examined to verify firmware on wireless devices is updated to support strong encryption for: • Authentication over wireless networks • Transmission over wireless networks	*Not Applicable*					
	Describe how wireless configuration settings verified that firmware on wireless devices is updated to support strong encryption for:						
	• Authentication over wireless networks.	*Not Applicable*					
	• Transmission over wireless networks.	*Not Applicable*					
2.1.1.e Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.	**Identify vendor documentation** examined to verify other security-related wireless vendor defaults were changed, if applicable.	*Not Applicable*					
	Describe how wireless configuration settings verified that other security-related wireless vendor defaults were changed, if applicable.	*Not Applicable*					
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)			☒	☐	☐	☐	☐
2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	**Identify the documented system configuration standards** for all types of system components examined to verify the system configuration standards are consistent with industry-accepted hardening standards.	*Doc-2* *Doc-4* *Doc-6* *Doc-13*					
	Provide the name of the assessor who attests that the system configuration standards are consistent with industry-accepted hardening standards.	*David M Dennis*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.b Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.	**Identify the policy documentation** examined to verify that system configuration standards are updated as new vulnerability issues are identified.	*Doc-1*					
	Identify the responsible personnel interviewed who confirm that system configuration standards are updated as new vulnerability issues are identified.	*Int-1* *Int-3* *Int-7* *Int-9*					
2.2.c Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.	**Identify the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network	*Doc-2* *Doc-4* *Doc-6* *Doc-13*					
	Identify the responsible personnel interviewed who confirm that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.	*Int-1* *Int-3* *Int-7* *Int-9*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.d Verify that system configuration standards include the following procedures for all types of system components: • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure • Configuring system security parameters to prevent misuse • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers	**Identify the system configuration standards** for all types of system components that include the following procedures: • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure • Configuring system security parameters to prevent misuse • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers	*Doc-2* *Doc-4* *Doc-6* *Doc-13*				
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*			☒	☐	☐	☐	☐
2.2.1.a Select a sample of system components and inspect the system configurations to verify that only one	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-6* *Sample Set-7* *Sample Set-8*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
primary function is implemented per server.	*For each item in the sample*, **describe how** system configurations verified that only one primary function per server is implemented.	*I observed by interview with Int-1 and observation of build document Doc-2 that Sangoma is following a process. I observed checklists involved and found that Sangoma defined specific build standards per server function, and that one function only was used per server.* *I observed in Sample Set-6 that the running processes on each Fedora server are determined by role. A syslog server had different file server mount point than a Jump box server, for example.* *I observed with assistance from Int-7 that the BIND server (Sample Set-7) was running the DNS daemon "BIND," and that there was a configuration file to match Sangoma' local DNS. Int-1 explained that the Sangoma server also acted as a resolver and forwarder, and I was shown the root server configuration which used the expected root server configuration required by most DNS resolvers.* *I observed the Sample Set-8 Jump Stations were set up differently than other servers, with no home directory space and a running-process configuration that was "stripped down," according to Int-1. I observed that no DNS and no syslog mount points were a part of this server's running configuration.* *In all, I observed each server class had a role that was described by Int-1, and that they were different. This led to a determination of compliance.*					
2.2.1.b If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device.	**Indicate whether** virtualization technologies are used. **(yes/no)**	*yes*					
	If "no," **describe how** systems were observed to verify that no virtualization technologies are used.	*Not Applicable*					
	If "yes":						
	Identify the sample of virtual system components or devices selected for this testing procedure.	*Sample Set-1*					
	For each virtual system component and device in the sample, **describe how** system configurations verified that only one primary function is implemented per virtual system component or device.	*I observed with assistance from Int-1 and Int-3 that each VDOM is assigned to a unique customer. I reviewed configuration to observe that VDOM cannot be used for multiple purposes, and that no VDOM are shared.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.2.a Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-5* *Sample Set-6* *Sample Set-7* *Sample Set-8*					
	For each item in the sample, **describe how** the enabled system services, daemons, and protocols verified that only necessary services or protocols are enabled.	*I reviewed output of running processes during live Zoom session that Int-1 performed by logging into servers in Sample Set-5, Sample Set-6, Sample Set-7 and Sample Set-8, which included the following outputs provided per each server observed:* • *Network interfaces information* • *Hostname* • *Open connections and listening ports* • *Mounted file systems* • *SSH v2 configuration* • *Sudoers* • *System authentication settings* • *Username list (/etc/passwd and sanitized /etc/shadow)* • *Log configurations* • *NTP settings* • *Running processes* • *iptables ruleset* • *Date of last password changes* *These data points were reviewed against prior knowledge and by what Int-1 described and compared to Doc-2 for what is expected for a Linux server running one service or one primary function, and also compared against the documented necessary services. All servers were observed to be built to the same operating system standards, same logging standards, and with the same hardening standards. This led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.2.b Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.	*For each item in the sample of system components from 2.2.2.a,* **indicate whether** any insecure services, daemons, or protocols are enabled. **(yes/no)** *If "no," mark the remainder of 2.2.2.b and 2.2.3 as "Not Applicable."*	*no*					
	If "yes," **identify the responsible personnel** interviewed who confirm that a documented business justification was present for each insecure service, daemon, or protocol	*Not Applicable. Sangoma does not run any insecure services, daemons or protocols.*					
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure			☐	☐	☒	☐	☐
2.2.3 Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols.	*If "yes" at 2.2.2.b, perform the following:*						
	Describe how configuration settings verified that security features for all insecure services, daemons, or protocols are:						
	• Documented	*Not Applicable. I reviewed Doc-6 and interviewed Int-1 and Int-2 to determine that Sangoma does not run any insecure services, daemons, or protocols.*					
	• Implemented	*Not Applicable*					
2.2.4 Configure system security parameters to prevent misuse.			☒	☐	☐	☐	☐
2.2.4.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.	**Identify the system administrators and/or security managers** interviewed for this testing procedure.	*Int-1* *Int-4*					
	For the interview, **summarize the relevant details** discussed to verify that they have knowledge of common security parameter settings for system components.	*I interviewed Int-1 and Int-4 who described the configuration details of the servers in Sangoma environment, such as hardening /etc/inetd.conf, and that this process, as well as the process of disabling unneeded accounts, running services as the role account rather than as root, and iptables to limit connections to only trusted local hosts on the local VLAN, are performed on the servers in Sample Set-4. This matched knowledge needed to support these environments.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.4.b Examine the system configuration standards to verify that common security parameter settings are included.	**Identify the system configuration standards** examined to verify that common security parameter settings are included.	*Doc-2*					
2.2.4.c Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-5* *Sample Set-6* *Sample Set-7* *Sample Set-8*					
	For each item in the sample, **describe how** the common security parameters verified that they are set appropriately and in accordance with the configuration standards.	*I observed during live Zoom session in Sample Set-5, Sample Set-6 Sample Set-7 and Sample Set-8 with assistance from Int-1 logging in and showing configuration files, that SSH v2 was configured not to allow remote root. SSH v2 was configured to only allow connections from trusted hosts on local VLAN. SSH v2 was configured to authenticated against LDAP, which is the Sangoma authentication user store, and is using role-based access based on the 'wheel' account for Administrators. Web ports 80/443 were only configured on www servers. Unneeded protocols were not enabled on any server. IP Tables were enabled on all servers, and the iptables configuration list was limited to trusted hosts and protocols. Time services are configured on all servers identically.*					
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.			☒	☐	☐	☐	☐
2.2.5.a Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-5* *Sample Set-6* *Sample Set-7* *Sample Set-8*					
	For each item in the sample, **describe how** configurations verified that all unnecessary functionality is removed.	*The scripted output of the servers in the sample was reviewed, and found to be the same for every server in each sample set. All servers in Sample Set-5, Sample Set-6, Sample Set-7 and Sample Set-8 were found to not be running common "extra" linux services in /etc/inetd.conf . All servers were found not to be running extra portmap services.*					
	Describe how the security parameters and relevant documentation verified that enabled functions are:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.2.5.b Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration.	• Documented	*The default server configuration in Doc-2 was reviewed against the output of the appropriate server commands observed during live Zoom review, and the output from the servers in Sample Set-5, Sample Set-6, Sample Set-7 and Sample Set-8 was found to have been limited to only those services that fit the policy.*					
	• Support secure configuration	*The Sample Set-5, Sample Set-6, Sample Set-7 and Sample Set-8 servers support SSH v2 only, and do not allow unsafe protocols such as Telnet, as these services are not running.*					
2.2.5.c Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components.	**Identify documentation** examined for this testing procedure.	*Doc-2*					
	Describe how the security parameters verified that only documented functionality is present on the sampled system components from 2.2.5.a.	*IP Tables trusted host list on the servers was limited to only ports and protocols needed for the server to do its job, e.g., SSH v2 server port, 80in the case of jump-servers. SSH v2 was configured to use pamd.conf and ssl.conf only.*					
2.3 Encrypt all non-console administrative access using strong cryptography.			☒	☐	☐	☐	☐
2.3 Select a sample of system components and verify that non-console administrative access is encrypted by performing the following:	**Identify the sample** of system components selected for 2.3.a-2.3.d.	*Sample Set-1* *Sample Set-4*					
2.3.a Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.	*For each item in the sample from 2.3:*						
	Describe how the administrator log on to each system verified that a strong encryption method is invoked before the administrator's password is requested.	*I observed during live Zoom session Int-1 access Sample Set-1 FortiGate using FortiClient from his administrative workstation/laptop. I observed that the certificate details provided in the client were TLS v1.2 AES 256-bit with high encryption set and a 2048-bit certificate.* *I observed SSH v2 sessions provided by Int-1 demonstration had key using RSA 2048-bit encryption.* *I observed Int-1 access Sample Set-4 using SSH v2 and observed the certificate. The certificate details were shown as TLS v1.2 / RSA 2048-bit.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how system configurations for each system verified that a strong encryption method is invoked before the administrator's password is requested.	*I asked Int-1 to show certificate on login session for FortiGate 1500D firewall and confirm the certificate details during live Zoom session. I observed that TLS v1.2 AES 256-bit with high encryption set and a 2048-bit was in place on every test case. I requested Int-1 provide SSH v2 details of login session by initiating a new key exchange, which I observed during Sample Set-4 testing. In every case observed the SSH v2 key was RSA 2048-bit.*					
	Identify the strong encryption method used for non-console administrative access.	*TLS v1.2 AES 256-bit with high encryption set and a 2048-bit certificate* *SSH v2/ RSA 2048-bit*					
2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.	*For each item in the sample from 2.3:*						
	Describe how services and parameter files on systems verified that Telnet and other insecure remote-login commands are not available for non-console access.	*I requested and obtained from Int-1 outputs of running processes on servers and FortiGate devices. I observed that Telnet, FTP, and other insecure services were not running in any of the outputs observed. I observed administrator using SSH v2 to access the servers in the sample set. I observed with assistance from Int-5 that SSH v2 is configured using RSA 2048 / Blowfish by displaying appropriate sshd.conf file on screen as part of the exercise of assembling Sample Set-8.*					
2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.	*For each item in the sample from 2.3:*						
	Describe how the administrator log on to each system verified that administrator access to any web-based management interfaces was encrypted with strong cryptography.	*Not Applicable. There are no web-based management interfaces in use, which was verified by observation of Int-1 accessing the servers in the sample set only by SSH v2 (Secure Shell) CLI (Command Line Interface) session. The administrator also confirmed verbally that no web-based management is enabled for the servers. To further illustrate the point, a https:// session (secure HTTP over port 443) connection was attempted to be executed by the administrator, and the session timed out without completing, indicative of a session which does not have support, e.g. would not work because it is not enabled.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the strong encryption method used for any web-based management interfaces.	*Not Applicable. There are no web-based management interfaces in use , which was verified by observation of Int-1 accessing the servers in the sample set only by SSH v2 (Secure Shell) CLI (Command Line Interface) session. The administrator also confirmed verbally that no web-based management is enabled for the servers. To further illustrate the point, a https:// session (secure HTTP over port 443) connection was attempted to be executed by the administrator, and the session timed out without completing, indicative of a session which does not have support, e.g. would not work because it is not enabled.*					
2.3.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	**Identify the vendor documentation** examined to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	*http://www.openssh.com/manual.html*					
	Identify the responsible personnel interviewed who confirm that that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	*Int-1*					
2.4 Maintain an inventory of system components that are in scope for PCI DSS.			☒	☐	☐	☐	☐
2.4.a Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.	**Describe how** the system inventory verified that a list of hardware and software components is:						
	• Maintained	*I read the inventory document (Doc-14) provided by Sangoma and observed that it matches the sampled hardware and software, as well as the names of devices in those samples.*					
	• Includes a description of function/use for each	*I read the inventory document (Doc-14) provided by Sangoma and observed that it matches the sampled hardware and software in the enterprise. I observed that Doc-14 contains descriptions of software in use and servers in use in Sangoma environment.*					
2.4.b Interview personnel to verify the documented inventory is kept current.	**Identify the responsible personnel** interviewed who confirm that the documented inventory is kept current.	*Int-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
2.5 Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for managing vendor defaults and other security parameters are documented.	*Doc-1*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for managing vendor defaults and other security parameters are: • In use • Known to all affected parties	*Int-1*					
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.*			☐	☐	☒	☐	☐
2.6 Perform testing procedures **A1.1** through **A1.4** detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.	**Indicate whether** the assessed entity is a shared hosting provider. **(yes/no)**	*no*					
	If "yes," **provide the name of the assessor** who attests that Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers has been completed.	*Not Applicable. Sangoma is not a shared hosting provider.*					

Protect Stored Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.1 Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed. • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.			☒	☐	☐	☐	☐
3.1.a Examine the data-retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. • Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). • Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	**Identify the data-retention and disposal documentation** examined to verify policies, procedures, and processes define the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements for data retention. • Specific requirements for retention of cardholder data. • Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons. • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	*Doc-1* *Doc-3*				

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.1.b Interview personnel to verify that: • All locations of stored cardholder data are included in the data-retention and disposal processes. • Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. • The quarterly automatic or manual process is performed for all locations of cardholder data.	**Identify the responsible personnel** interviewed who confirm that: • All locations of stored cardholder data are included in the data-retention and disposal processes. • Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. • The quarterly automatic or manual process is performed for all locations of cardholder data.	*Int-1* *Int-2*					
3.1.c For a sample of system components that store cardholder data: • Examine files and system records to verify that the data stored does not exceed the requirements defined in the data-retention policy. • Observe the deletion mechanism to verify data is deleted securely.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-4*					
	For each item in the sample, **describe how** files and system records verified that the data stored does not exceed the requirements defined in the data-retention policy.	*I observed during live Zoom review with assistance from Int-1 of Sample Set-4, and observed no databases or cardholder data storage on any of the servers. I reviewed Doc-42, Doc-43, and Doc-44 and observed that no database servers existed. I then reviewed Doc-18 and observed that there is no risk of cardholder data loss in Sangoma' risk plan, and that the risk involving any cardholder data was defined as belonging to the customer, if they had any CHD at all. I was able to determine that Sangoma does not store, process or forward cardholder data. However, Sangoma maintains a data review process as documented in their policies. This includes a review for out-of-scope potential for cardholder data. Data retention and disposal is included in their policies.*					
	Describe how the deletion mechanism was observed to verify data is deleted securely.	*Not Applicable. I observed by interview with Int-1 and review of Doc-18, Doc-42, Doc-43, and Doc-44, as well as live Zoom remote session review of Sample Set-4 that Sangoma had no cardholder data storage and as a result no cardholder data deletion.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* • *There is a business justification, and* • *The data is stored securely.* *Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:*			☐	☐	☒	☐	☐
3.2.a For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.	**Indicate whether** the assessed entity is an issuer or supports issuing service. **(yes/no)**	*no*					
	If "yes," complete the responses for 3.2.a and 3.2.b and mark 3.2.c and 3.2.d as "Not Applicable." *If "no," mark the remainder of 3.2.a and 3.2.b as "Not Applicable" and proceed to 3.2.c and 3.2.d.*						
	Identify the documentation reviewed to verify there is a documented business justification for the storage of sensitive authentication data.	*Not Applicable*					
	Identify the interviewed personnel who confirm there is a documented business justification for the storage of sensitive authentication data.	*Not Applicable*					
	For the interview, **summarize the relevant details** of the business justification described.	*Not Applicable*					
3.2.b For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured.	*If "yes" at 3.2.a,*						
	Identify data stores examined.	*Not Applicable*					
	Describe how the data stores and system configurations were examined to verify that the sensitive authentication data is secured.	*Not Applicable*					
3.2.c For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.	**Indicate whether** sensitive authentication data is received. **(yes/no)**	*no*					
	If "yes," complete 3.2.c and 3.2.d. *If "no," mark the remainder of 3.2.c and 3.2.d as "Not Applicable" and proceed to 3.2.1.*						
	Identify the document(s) reviewed to verify the data is not retained after authorization.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Describe how system configurations verified that the data is not retained after authorization.	*Not Applicable*					
3.2.d For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable.	**Identify the document(s)** reviewed to verify that it defines processes for securely deleting the data so that it is unrecoverable.	*Not Applicable*					
	Describe how the processes for securely deleting the data were examined to verify that the data is unrecoverable.	*Not Applicable*					
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*			☒	☐		☐	☐
3.2.1 For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error)	**Identify the sample** of system components selected for 3.2.1-3.2.3.	*Sample Set-5* *Sample Set-6* *Sample Set-7* *Sample Set-8*					
	For each data source type below from the sample of system of components examined, **summarize the specific examples of each data source type observed** to verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization. If that type of data source is not present, indicate that in the space.						
	• Incoming transaction data	*Not Present*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• History files • Trace files • Several database schemas • Database contents	• All logs (for example, transaction, history, debugging error)	*207.232.81.142 (Logfile; no extension used by Sangoma for this log filename)* *207.232.82.142 (Logfile; no extension used by Sangoma for this log filename* *207.232.81.169 (Logfile; no extension used by Sangoma for this log filename)* *69.168.216.216 (Logfile; no extension used by Sangoma for this log filename)* *74.85.31.110 (Logfile; no extension used by Sangoma for this log filename)* *Tac_plus.acct (Logfile; no extension used by Sangoma for this log filename)* *Tacplus-do_auth.log*					
	• History files	*Not Present*					
	• Trace files	*Not Present*					
	• Database schemas	*Not Present*					
	• Database contents	*Not Present*					
	• If applicable, **any other output observed** to be generated	*Not Applicable*					
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization.			☒	☐		☐	☐
3.2.2 For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2,	*For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. If that type of data source is not present, indicate that in the space.						
	• Incoming transaction data	*Not Present*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
CID, CAV2 data) is not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents	• All logs (for example, transaction, history, debugging error)	*207.232.81.142 (Logfile; no extension used by Sangoma for this log filename)* *207.232.82.142 (Logfile; no extension used by Sangoma for this log filename)* *207.232.81.169 (Logfile; no extension used by Sangoma for this log filename)* *69.168.216.216 (Logfile; no extension used by Sangoma for this log filename)* *74.85.31.110 (Logfile; no extension used by Sangoma for this log filename)* *Tac_plus.acct (Logfile; no extension used by Sangoma for this log filename)* *Tacplus-do_auth.log*					
	• History files	*Not Present*					
	• Trace files	*Not Present*					
	• Database schemas	*Not Present*					
	• Database contents	*Not Present*					
	• If applicable, **any other output observed** to be generated	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.			☒	☐		☐	☐
3.2.3 For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents	*For each data source type below from the sample of system of components at 3.2.1,* **summarize the specific examples of each data source type observed** to verify that PINs and encrypted PIN blocks are not stored after authorization. If that type of data source is not present, indicate that in the space.						
	• Incoming transaction data	*Not Present*					
	• All logs (for example, transaction, history, debugging error)	*207.232.81.142 (Logfile; no extension used by Sangoma for this log filename)* *207.232.82.142 (Logfile; no extension used by Sangoma for this log filename)* *207.232.81.169 (Logfile; no extension used by Sangoma for this log filename)* *69.168.216.216 (Logfile; no extension used by Sangoma for this log filename)* *74.85.31.110. (Logfile; no extension used by Sangoma for this log filename)* *Tac_plus.acct (Logfile; no extension used by Sangoma for this log filename)* *Tacplus-do_auth.log*					
	• History files	*Not Present*					
	• Trace files	*Not Present*					
	• Database schemas	*Not Present*					
	• Database contents	*Not Present*					
	• If applicable, **any other output observed** to be generated	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN. ***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*			☐	☐	☒	☐	☐
3.3.a Examine written policies and procedures for masking the display of PANs to verify: • A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	**Identify the document(s)** reviewed to verify that written policies and procedures for masking the displays of PANs include the following: • A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	*Not Applicable. Cardholder data if present is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*				
3.3.b Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests.	**Describe how** system configurations verified that:						
	• Full PAN is only displayed for users/roles with a documented business need.	*Not Applicable. I read Doc-3 and Doc-18 and interviewed Int-1 to learn that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*					
	• PAN is masked for all other requests.	*Not Applicable*					
3.3.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are	**Describe how** displays of PAN verified that:						
	• PANs are masked when displaying cardholder data.	*Not Applicable. I read Doc-3 and Doc-18, and interviewed Int-1 to learn that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
able to see more than first six/last four digits of the PAN.	• Only those with a legitimate business need are able to see more than first six/last four digits of the PAN.	*Not Applicable*					
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN). • Truncation (hashing cannot be used to replace the truncated segment of PAN). • Index tokens and pads (pads must be securely stored). • Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*			☐	☐	☒	☐	☐
3.4.a Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography, • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	**Identify the documentation** examined to verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography, • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	*Not Applicable. I read Doc-3, and Doc-23 and interviewed Int-1 to determine that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).	**Identify the sample** of data repositories selected for this testing procedure.	*Not Applicable*					
	Identify the tables or files examined for each item in the sample of data repositories.	*Not Applicable*					
	For each item in the sample, **describe how** the tables or files verified that the PAN is rendered unreadable.	*Not Applicable*					
3.4.c Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable.	**Identify the sample** of removable media selected for this testing procedure.	*Not Applicable*					
	For each item in the sample, **describe how** the sample of removable media confirmed that the PAN is rendered unreadable.	*Not Applicable*					
3.4.d Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs.	**Identify the sample** of audit logs, including payment application logs, selected for this testing procedure.	*Not Applicable*					
	For each item in the sample, **describe how** the sample of audit logs, including payment application logs, confirmed that the PAN is rendered unreadable or is not present in the logs.	*Not Applicable*					
3.4.e If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	**Identify whether** hashed and truncated versions of the same PAN are present in the environment **(yes/no)** *If 'no,'* mark 3.4.e as 'not applicable' and proceed to 3.4.1.	*Not Applicable*					
	If 'yes,' **describe** the implemented controls examined to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	*Not Applicable*					
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. *Note: This requirement applies in addition to all other PCI DSS encryption and key management requirements.*			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.4.1.a If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials).	**Indicate whether** disk encryption is used. **(yes/no)**	*no*					
	If "yes," complete the remainder of 3.4.1.a, 3.4.1.b, and 3.4.1.c. *If "no," mark the remainder of 3.4.1.a, 3.4.1.b and 3.4.1.c as "Not Applicable."*						
	Describe the disk encryption mechanism(s) in use.	*Not Applicable*					
	For each disk encryption mechanism in use, **describe how** the configuration verified that logical access to encrypted file systems is separate from the native operating system's authentication mechanism.	*Not Applicable*					
	For each disk encryption mechanism in use, **describe how** the authentication process was observed to verify that logical access to encrypted file systems is separate from the native operating system's authentication mechanism.	*Not Applicable*					
3.4.1.b Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	**Describe how** processes were observed to verify that cryptographic keys are stored securely.	*Not Applicable*					
	Identify the responsible personnel interviewed who confirm that cryptographic keys are stored securely.	*Not Applicable*					
3.4.1.c Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored. ***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*	**Describe how** the configurations verified that cardholder data on removable media is encrypted wherever stored.	*Not Applicable*					
	Describe how processes were observed to verify that cardholder data on removable media is encrypted wherever stored.	*Not Applicable*					
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.5 Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	**Identify the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	*Not Applicable. I read Doc-3 and Doc-23, and interviewed Int-1 to determine that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*					
3.5.1 ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management			☐	☐	☒	☐	☐
3.5.1 Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date	**Identify the responsible personnel interviewed** who confirm that a document exists to describe the cryptographic architecture, including: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management	*Not Applicable. I read Doc-3 and Doc-23 and interviewed Int-1 to determine that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management	**Identify the documentation reviewed** to verify that it contains a description of the cryptographic architecture, including: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management	*Not Applicable*					
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.			☐	☐	☒	☐	☐
3.5.2 Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	**Identify user access lists** examined.	*Not Applicable. I read Doc-3 and Doc-23 and interviewed Int-1 to determine that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*					
	Describe how the user access lists verified that access to keys is restricted to the fewest number of custodians necessary.	*Not Applicable*					
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). • As at least two full-length key components or key shares, in accordance with an industry-accepted method. ***Note:*** *It is not required that public keys be stored in one of these forms.*			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.5.3.a Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). • As key components or key shares, in accordance with an industry-accepted method.	**Identify the documented procedures** examined to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). • As key components or key shares, in accordance with an industry-accepted method.	*Not Applicable. I read Doc-3 and Doc-23 and interviewed Int-1 and determined that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*				
3.5.3.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one, (or more), of the following form at all times. • Encrypted with a key-encrypting key. • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). • As key components or key shares, in accordance with an industry-accepted method.	**Provide the name of the assessor** who attests that all locations where keys are stored were identified.	*Not Applicable*					
	Describe how system configurations and key storage locations verified that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device). • As key components or key shares, in accordance with an industry-accepted method.	*Not Applicable*					
3.5.3.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify:	**Describe how** system configurations and key storage locations verified that, wherever key-encrypting keys are used:						
	• Key-encrypting keys are at least as strong as the data-encrypting keys they protect.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys.	• Key-encrypting keys are stored separately from data-encrypting keys.	*Not Applicable*					
3.5.4 Store cryptographic keys in the fewest possible locations.			☐	☐	☒	☐	☐
3.5.4 Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	**Describe how** key storage locations and the observed processes verified that keys are stored in the fewest possible locations.	*Not Applicable. I read Doc-3 and Doc-23 and interviewed Int-1 to determine that cardholder data is the responsibility of Sangoma customers, as defined by review of Doc-3 and Doc-18 and confirmed by interview with Int-1.*					
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*			☐	☐	☒	☐	☐
3.6.a ***Additional Procedure for service provider assessments only***: If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers' keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	**Indicate whether** the assessed entity is a service provider that shares keys with their customers for transmission or storage of cardholder data. **(yes/no)**	*no*					
	If "yes," **Identify the document** that the service provider provides to their customers examined to verify that it includes guidance on how to securely transmit, store and update customers' keys, in accordance with Requirements 3.6.1 through 3.6.8 below.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider that provides data transit connectivity only, and that they do not share keys with customers for transmission or storage of cardholder data.*					
3.6.b Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following:							
3.6.1 Generation of strong cryptographic keys.			☐	☐	☒	☐	☐
3.6.1.a Verify that key-management procedures specify how to generate strong keys.	**Identify the documented key-management procedures** examined to verify procedures specify how to generate strong keys.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider, they do not generate keys with customers for transmission or storage of cardholder data.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.1.b Observe the procedures for generating keys to verify that strong keys are generated.	**Describe how** the procedures for generating keys were observed to verify that strong keys are generated.	*Not Applicable*					
3.6.2 Secure cryptographic key distribution.			☐	☐	☒	☐	☐
3.6.2.a Verify that key-management procedures specify how to securely distribute keys.	**Identify the documented key-management procedures** examined to verify procedures specify how to securely distribute keys.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider, they do not distribute keys with customers for transmission or storage of cardholder data.*					
3.6.2.b Observe the method for distributing keys to verify that keys are distributed securely.	**Describe how** the method for distributing keys was observed to verify that keys are distributed securely.	*Not Applicable*					
3.6.3 Secure cryptographic key storage.			☐	☐	☒	☐	☐
3.6.3.a Verify that key-management procedures specify how to securely store keys.	**Identify the documented key-management procedures** examined to verify procedures specify how to securely store keys.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider, they do not store keys for customers for transmission or storage of cardholder data.*					
3.6.3.b Observe the method for storing keys to verify that keys are stored securely.	**Describe how** the method for storing keys was observed to verify that keys are stored securely.	*Not Applicable*					
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).			☐	☐	☒	☐	☐
3.6.4.a Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s).	**Identify the documented key-management procedures** examined to verify procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s).	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider, they do not share keys with customers for transmission or storage of cardholder data.*					
3.6.4.b Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s).	**Identify** the responsible **personnel interviewed** who confirm that keys are changed at the end of the defined cryptoperiod(s).	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*			☐	☐	☒	☐	☐
3.6.5.a Verify that key-management procedures specify processes for the following: • The retirement or replacement of keys when the integrity of the key has been weakened. • The replacement of known or suspected compromised keys. • Any keys retained after retiring or replacing are not used for encryption operations.	**Identify the documented key-management procedures** examined to verify that key-management processes specify the following: • The retirement or replacement of keys when the integrity of the key has been weakened. • The replacement of known or suspected compromised keys. • Any keys retained after retiring or replacing are not used for encryption operations.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider they do not share keys with customers for transmission or storage of cardholder data, and as a result do not retire any keys of this type.*					
3.6.5.b Interview personnel to verify the following processes are implemented: • Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. • Keys are replaced if known or suspected to be compromised. • Any keys retained after retiring or replacing are not used for encryption operations.	**Identify the responsible personnel** interviewed who confirm that the following processes are implemented: • Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. • Keys are replaced if known or suspected to be compromised. • Any keys retained after retiring or replacing are not used for encryption operations.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider, they do not share keys with customers for transmission or storage of cardholder data and as a result, do not retire any keys of this type.*					
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. ***Note:*** Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.			☐	☐	☒	☐	☐
	Indicate whether manual clear-text cryptographic key-management operations are used. **(yes/no)**	*no*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.6.a Verify that manual clear-text key-management procedures specify processes for the use of the following: • Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND • Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another.	*If "no," mark the remainder of 3.6.6.a and 3.6.6.b as "Not Applicable."* *If "yes," complete 3.6.6.a and 3.6.6.b.*						
	Identify the documented key-management procedures examined to verify that manual clear-text key-management procedures define processes for the use of the following: • Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND • Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials of another.	*Not Applicable*					
3.6.6.b Interview personnel and/or observe processes to verify that manual clear-text keys are managed with: • Split knowledge, AND • Dual control	**Identify the responsible personnel** interviewed for this testing procedure, if applicable.	*Not Applicable*					
	For the interview, **summarize the relevant details discussed and/or describe how** processes were observed to verify that manual clear-text keys are managed with:						
	• Split knowledge	*Not Applicable*					
	• Dual Control	*Not Applicable*					
3.6.7 Prevention of unauthorized substitution of cryptographic keys.			☐	☐	☒	☐	☐
3.6.7.a Verify that key-management procedures specify processes to prevent unauthorized substitution of keys.	**Identify the documented key-management procedures** examined to verify that key-management procedures specify processes to prevent unauthorized substitution of keys.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider, they do not share keys with customers for transmission or storage of cardholder data.*					
3.6.7.b Interview personnel and/or observe process to verify that unauthorized substitution of keys is prevented.	**Identify the responsible personnel** interviewed for this testing procedure, if applicable.	*Not Applicable*					
	For the interview, **summarize the relevant details discussed and/or describe how** processes were observed to verify that unauthorized substitution of keys is prevented.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.			☐	☐	☒	☐	☐
3.6.8.a Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**Identify the documented key-management procedures** examined to verify that key-management procedures specify processes for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.	*Not Applicable. I determined from review of policies (Doc-1, Doc-2, and Doc-6) and interviewees (Sample Set-14, Sample Set-15) that while Sangoma is a service provider, they do not share keys with customers for transmission or storage of cardholder data, thus do not have key custodians for this role.*					
3.6.8.b Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**Describe how** key custodian acknowledgements or other evidence were observed to verify that key custodians have acknowledged that they understand and accept their key-custodian responsibilities.	*Not Applicable*					
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
3.7 Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are: • Documented, • In use, and • Known to all affected parties	**Identify the document** reviewed to verify that security policies and operational procedures for protecting stored cardholder data are documented.	*Doc-1* *Doc-3*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for protecting stored cardholder data are: • In use • Known to all affected parties	*Int-1* *Int-3*					

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *Examples of open, public networks include but are not limited to:* • *The Internet* • *Wireless technologies, including 802.11 and Bluetooth* • *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* • *General Packet Radio Service (GPRS)* • *Satellite communications*			☐	☐	☒	☐	☐
4.1.a Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.	**Identify** all locations where cardholder data is transmitted or received over open, public networks.	*Not Applicable. I determined by interview with Int-1 and review of Doc-42, Doc-43 and Doc-44 that Sangoma does not transmit cardholder data over open, public networks. Sangoma maintains these configurations to protect administrative access for itself, and to separate its administrative duties from potentially impacting security of the defined transit network*					
	Identify the documented standards examined.	*Not Applicable*					
	Describe how the documented standards and system configurations both verified the use of:						
	• Security protocols for all locations	*Not Applicable*					
	• Strong cryptography for all locations	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
4.1.b Review documented policies and procedures to verify processes are specified for the following: • For acceptance of only trusted keys and/or certificates. • For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). • For implementation of proper encryption strength per the encryption methodology in use.	**Identify the document** reviewed to verify that processes are specified for the following: • For acceptance of only trusted keys and/or certificates. • For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). • For implementation of proper encryption strength per the encryption methodology in use.	*Not Applicable*					
4.1.c Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit.	**Describe the sample** of inbound and outbound transmissions that were observed as they occurred.	*Not Applicable*					
	Describe how the sample of inbound and outbound transmissions verified that all cardholder data is encrypted with strong cryptography during transit.	*Not Applicable*					
4.1.d Examine keys and certificates to verify that only trusted keys and/or certificates are accepted.	*For all instances where cardholder data is transmitted or received over open, public networks:*						
	Describe the mechanisms used to ensure that only trusted keys and/or certificates are accepted.	*Not Applicable*					
	Describe how the mechanisms were observed to accept only trusted keys and/or certificates.	*Not Applicable*					
4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.	*For all instances where cardholder data Is transmitted or received over open, public networks,* **describe how** system configurations verified that the protocol:						
	• Is implemented to use only secure configurations.	*Not Applicable*					
	• Does not support insecure versions or configurations.	*Not Applicable*					
4.1.f Examine system configurations to verify that the proper encryption strength is implemented for the encryption	*For each encryption methodology in use,*						
	Identify vendor recommendations/best practices for encryption strength.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
methodology in use. (Check vendor recommendations/best practices.)	**Identify** the encryption strength observed to be implemented.	*Not Applicable*					
4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received. *For example, for browser-based implementations:* • *"HTTPS" appears as the browser Universal Record Locator (URL) protocol; and* • *Cardholder data is only requested if "HTTPS" appears as part of the URL.*	**Indicate whether** TLS is implemented to encrypt cardholder data over open, public networks. **(yes/no)** *If 'no,' mark the remainder of 4.1.g as 'not applicable.'*	*Not Applicable*					
	If "yes," for all instances where TLS is used to encrypt cardholder data over open, public networks, **describe how** system configurations verified that TLS is enabled whenever cardholder data is transmitted or received.	*Not Applicable*					
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.			☐	☐	☒	☐	☐
4.1.1 Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified: • Industry best practices are used to implement strong encryption for authentication and transmission. • Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission.	**Identify** all wireless networks transmitting cardholder data or connected to the cardholder data environment.	*Not Applicable. I confirmed by review of Doc-20, Doc-42, Doc-43 and Doc-44 that Sangoma does not connect any wireless to the data environment, and that the data environment does not transmit cardholder data over wireless networks.*					
	Identify the documented standards examined.	*Not Applicable*					
	Describe how the documented standards and system configuration settings both verified the following for all wireless networks identified:						
	• Industry best practices are used to implement strong encryption for authentication and transmission.	*Not Applicable*					
	• Weak encryption is not used as a security control for authentication or transmission.	*Not Applicable*					
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
4.2.a If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	**Indicate whether** end-user messaging technologies are used to send cardholder data. **(yes/no)**	*no*					
	If "no," mark the remainder of 4.2.a as "Not Applicable" and proceed to 4.2.b. *If "yes," complete the following:*						
	Describe how processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	*Not Applicable. Sangoma does not use end-user messaging technologies to send cardholder data.*					
	Describe the sample of outbound transmissions that were observed as they occurred.	*Not Applicable*					
	Describe how the sample of outbound transmissions verified that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	*Not Applicable*					
4.2.b Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	**Identify the policy document** that prohibits PAN from being sent via end-user messaging technologies under any circumstances.	*Doc-1*					
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
4.3 Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for encrypting transmissions of cardholder data are documented.	*Doc-1* *Doc-25*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for encrypting transmissions of cardholder data are: • In use • Known to all affected parties	*Int-1*					

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).			☒	☐	☐	☐	☐
5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	**Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure.	*Sample Set-4* *Sample Set-9*					
	For each item in the sample, **describe how** anti-virus software was observed to be deployed.	*I observed installed FortiClient Endpoint Management Server (EMS) on Administrator workstations (Sample Set-9, Sample Set-4) observed during live Zoom session. I observed that the clients were installed on all devices and were running.*					
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.			☒	☐	☐	☐	☐
5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs; • Detect all known types of malicious software, • Remove all known types of malicious software, and • Protect against all known types of malicious software. *(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits).*	**Identify the vendor documentation** reviewed to verify that anti-virus programs: • Detect all known types of malicious software, • Remove all known types of malicious software, and • Protect against all known types of malicious software.	*Doc-15*					
	Describe how anti-virus configurations verified that anti-virus programs:						
	• Detect all known types of malicious software,	*I read the FortiClient Endpoint Management Server (EMS) 6.4.8.1755 screen shown by Int-1 during live Zoom session and saw that it is enabled. I read Doc-15 and found that EMS detects all known types of malicious software. I read the EMS client screen provided by Int-2, Int-3 and Int-4 and determined that they were enabled. I read Doc-15 and confirmed that EMS detects all known types of malicious software.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Remove all known types of malicious software, and	*I read the FortiClient Endpoint Management Server (EMS) 6.4.8.1755 screen shown by Int-1 during Zoom demonstration and saw that it is enabled. I read Doc-15 and found that EMS removes all known types of malicious software. I read the EMS client screen provided by Int-2, Int-3 and Int-4 and determined that they were enabled.*					
	• Protect against all known types of malicious software.	*I read the EMS screen shown by Int-1 during Zoom session and saw that it is enabled. I read Doc-15 and found that EMS protects against all types of malicious software. I read the EMS client screen provided by Int-2, Int-3 and Int-4 and determined that they were enabled.*					
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.			☒	☐	☐	☐	☐
5.1.2 Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.	**Identify the responsible personnel** interviewed for this testing procedure.	*Int-1* *Int-2* *Int-3*					
	For the interview, **summarize the relevant details discussed** to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, and that such systems continue to not require anti-virus software.	*I observed with assistance from Int-2 and Int-3 during Zoom session and review of Doc-2 that Sangoma builds Linux systems (Sample Set-4) with a ClamAV agent installed by default following ClamAV documentation (Doc-48). This agent is configured to receive updates daily and is configured to send alarm alerts to the system security group, of which Int-1, Int-2 and Int-3 are members. Sample Set-12 was created to illustrate these details and matches the evidence cited by Int-1, Int-2 and Int-3.*					
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current. • Perform periodic scans. • Generate audit logs which are retained per PCI DSS Requirement 10.7.			☒	☐	☐	☐	☐
5.2.a Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up-to-date.	**Identify the documented policies and procedures** examined to verify that anti-virus software and definitions are required to be kept up to date.	*Doc-1* *Doc-48*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.2.b Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans.	**Describe how** anti-virus configurations, including the master installation of the software, verified anti-virus mechanisms are:						
	• Configured to perform automatic updates, and	*I observed Int-1 during a live Zoom review of sampled servers (Sample Set-4) and show the ClamAV update script and update directory on the servers to me for review. As a result of this, I was able to see that the process of install sets up ClamAV using freshclam to update ClamDB, part of the ClamAV suite, daily. This is part of the clamd process, which forks a freshclam instance on the servers, which indicates that a live ClamAV process is running.* *I observed during live Zoom Sample Set-9 computers were running EMS software, by observing Int-1, Int-2, Int-3 and Int-4 laptop workstations. The software had been updated within a few minutes of the time I had observed them, as shown in the "last updated" log.*					
	• Configured to perform periodic scans.	*I observed Int-1 during the Zoom session and live review open the /etc/cron.daily/clamscan_daily file, which is the configuration file for the ClamAV suite on the servers in Sample Set-4, and contained in the file were the lines of configuration that when compared to the ClamAV documentation said that the /etc/cron.daily/clamscan_daily is configured to scan servers in Sample Set-4 for daily updating.* *I observed in Sample Set-9 that the EMS clients were configured to scan the hard drives of Administrator workstation laptops daily.*					
5.2.c Examine a sample of system components, including all operating	**Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure.	*Sample Set-4* *Sample Set-9*					
	Describe how the system components verified that:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
system types commonly affected by malicious software, to verify that: • The anti-virus software and definitions are current. • Periodic scans are performed.	• The anti-virus software and definitions are current.	*I observed during the live session that Int-1 showed the aspects of ClamAV shown in Sample Set-4 and from those I confirmed cron job exists for all clamav installs, and that freshclam is running on all servers. I observed in Sample Set-9 that the client definitions were recent and the client pulling definitions from the FortiClient Endpoint Management Server (EMS) 6.4.8.1755 server sites were up to date.*					
	• Periodic scans are performed.	*I observed during live sessions with Int-1 that scans (the configurations from which were part of Sample Set-4) are configured in the daily or hourly cron job directories, to run at a minimum daily, and hourly on high-risk systems (public facing www systems). I observed in Sample Set-9 that recent AV scans had occurred by the "last scanned" date visible.*					
5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that: • Anti-virus software log generation is enabled, and • Logs are retained in accordance with PCI DSS Requirement 10.7.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-4*					
	For each item in the sample, **describe how** anti-virus configurations, including the master installation of the software, verified that:						
	• Anti-virus software log generation is enabled, and.	*During the review sessions conducted by live remote Zoom sessions with Int-1, I was shown ClamAV configuration directory and file. I was able to interview Int-1 to explain the configuration, who explained that ClamAV is configured to log using syslog under its standard method of operation, which is followed by Sangoma during installs following Doc-48.*					
	• Logs are retained in accordance with PCI DSS Requirement 10.7.	*All logging is sent to the central logging server, which holds logs for a period of a year in accordance with PCI-DSS 10.7 requirement. This was observed when Int-1 logged into servers in Sample Set-4 and I saw the configuration examples on the screen.*					
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.3.a Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-4*					
	For each item in the sample, **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software is actively running.	*I observed Int-1 log into servers during live Zoom session, and explain how clamd is configured. I was able to determine based on the knowledge here and in the Doc-48 manual that clamd and freshclam in active operation on all servers.*					
5.3.b Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users.	*For each item in the sample from 5.3.a,* **describe how** anti-virus configurations, including the master installation of the software, verified that the anti-virus software cannot be disabled or altered by users.	*I observed visually on the screen during the live Zoom session when Int-1 logged in and displayed the configuration on the screen that clamd and freshclam are installed with clam user permissions, which cannot be altered by non-administrative (root) users on the servers. In addition, cron job directories are not permissioned for non-privileged user access.*					
5.3.c Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	**Identify the responsible personnel** interviewed who confirm that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	*Int-1*					
	Describe how processes were observed to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	*This was observed by permissions 'rwx—x—x' on the cron job directories as part of the linux standard build in use by Sangoma under Doc-2, Doc-13. Users on these servers are also not granted permission to write to system binary directories.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
5.4 Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are: • Documented, • In use, and • Known to all affected parties.	**Identify the document reviewed to** verify that security policies and operational procedures for protecting systems against malware are documented.	*Doc-1* *Doc-2* *Doc-4* *Doc-13*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for protecting systems against malware are: • In use • Known to all affected parties	*Int-1* *Int-2* *Int-3*					

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*			☒	☐	☐	☐	☐
6.1.a Examine policies and procedures to verify that processes are defined for the following: • To identify new security vulnerabilities. • To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • To include using reputable outside sources for security vulnerability information.	**Identify the documented policies and procedures** examined to confirm that processes are defined: • To identify new security vulnerabilities. • To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • To include using reputable outside sources for security vulnerability information.	*Doc-19*					
6.1.b Interview responsible personnel and observe processes to verify that: • New security vulnerabilities are identified. • A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities.	**Identify the responsible personnel** interviewed who confirm that: • New security vulnerabilities are identified. • A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities. • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	*Int-1* *Int-2*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	**Describe how** processes were observed to verify that:						
	• New security vulnerabilities are identified.	*I observed during Zoom session with Int-1 demonstrating Nessus scan screen and prior findings files that were visible that Sangoma maintains Nessus scanning on at least a quarterly basis to identify new vulnerabilities on its environment.*					
	• A risk ranking is assigned to vulnerabilities to include identification of all "high" risk and "critical" vulnerabilities.	*I observed with assistance from Int-1 during live Zoom session that Sangoma uses the CVE ranking in use by Nessus and by vendor web sites to rank risks. In addition, there is a "low/medium/high" risk ranking in use for Sangoma' own risk ranking activities.*					
	• Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	*I observed that Sangoma watches security updates from Cisco, Red Hat, Fortinet, and from open-source tracking on the internet through sites like the Mitre.org CVE Database.*					
	Identify the outside sources used.	*Red Hat* *Cisco* *FortiNet* *Mitre.org* *SANS*					
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:*** *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*			☒	☐	☐	☐	☐
6.2.a Examine policies and procedures related to security-patch installation to verify processes are defined for: • Installation of applicable critical vendor-supplied security patches within one month of release. • Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).	**Identify the documented policies and procedures** related to security-patch installation examined to verify processes are defined for: • Installation of applicable critical vendor-supplied security patches within one month of release. • Installation of all applicable vendor-supplied security patches within an appropriate time frame.	*Doc-19*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.2.b For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following: • That applicable critical vendor-supplied security patches are installed within one month of release. • All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).	**Identify the sample** of system components and related software selected for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	Identify the vendor security patch list reviewed.	*Sample Set-13*					
	For each item in the sample, **describe how** the list of security patches installed on each system was compared to the most recent vendor security-patch list to verify that:						
	• Applicable critical vendor-supplied security patches are installed within one month of release.	*I compared the security patch list at Fedora Core (Sample Set-4), and FortiNet and Palo Alto vulnerabilities (Sample Set-1) to tickets for critical vulnerabilities in the previous year. The patching dates were within 30 days of the announcement of the vulnerability.*					
	• All applicable vendor-supplied security patches are installed within an appropriate time frame.	*I observed with assistance from Int-3 the FortiGate security critical patch upgrades from Fortinet and Palo Alto that included patches required for Sample Set-1 for critical vulnerabilities were installed within 30 days.* *I observed critical security patching from Red Hat with assistance from Int-1 and observed that the RPM versions and release dates matched what I observed in Sample Set-4*					
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging). • Based on industry standards and/or best practices. • Incorporate information security throughout the software development life cycle. ***Note**: this applies to all software developed internally as well as bespoke or custom software developed by a third party.*			☐	☐	☒	☐	☐
6.3.a Examine written software-development processes to verify that the processes are based on industry standards and/or best practices.	**Identify the document** examined to verify that software-development processes are based on industry standards and/or best practices.	*Not Applicable. I determined that, as a service provider, Sangoma does not provide development services or develop custom code in use in the in-scope environment. I reviewed Doc-23 and interviewed Int-1 to validate that this control is not applicable.*					
6.3.b Examine written software-development processes to verify that information security is included throughout the life cycle.	**Identify the documented software-development processes** examined to verify that information security is included throughout the life cycle.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.3.c Examine written software-development processes to verify that software applications are developed in accordance with PCI DSS.	**Identify the documented software-development processes** examined to verify that software applications are developed in accordance with PCI DSS.	*Not Applicable*					
6.3.d Interview software developers to verify that written software development processes are implemented.	**Identify the software developers** interviewed who confirm that written software-development processes are implemented.	*Not Applicable*					
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.			☐	☐	☒	☐	☐
6.3.1 Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	**Identify the documented software-development processes** examined to verify processes define that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	*Not Applicable. I learned by interview with Int-1 that, as a service provider, Sangoma does not provide development services or develop custom code in use in the in-scope environment.*					
	Identify the responsible personnel interviewed who confirm that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	*Not Applicable*					
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines. • Appropriate corrections are implemented prior to release. • Code review results are reviewed and approved by management prior to release. ***Note:*** *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.3.2.a Examine written software development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows: • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	**Identify the documented software-development processes** examined to verify processes define that all custom application code changes must be reviewed (using either manual or automated processes) as follows: • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	*Not Applicable. I learned by interview with Int-1 that Sangoma does not provide development services or develop custom code in use in the in-scope environment. I reviewed Doc-23 and interviewed Int-1 to validate that this control is not applicable.*					
	Identify the responsible personnel interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows: • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	*Not Applicable*					
6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.	**Identify the sample** of recent custom application changes selected for this testing procedure.	*Not Applicable*					
	For each item in the sample, **describe how** code review processes were observed to verify custom application code is reviewed as follows:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Code changes are reviewed by individuals other than the originating code author.	*Not Applicable*					
	• Code changes are reviewed by individuals who are knowledgeable in code-review techniques and secure coding practices.	*Not Applicable*					
	• Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5).	*Not Applicable*					
	• Appropriate corrections are implemented prior to release.	*Not Applicable*					
	• Code-review results are reviewed and approved by management prior to release.	*Not Applicable*					
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:			☒	☐	☐	☐	☐
6.4 Examine policies and procedures to verify the following are defined: • Development/test environments are separate from production environments with access control in place to enforce separation. • A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. • Production data (live PANs) are not used for testing or development. • Test data and accounts are removed before a production system becomes active. • Change control procedures related to implementing security patches and software modifications are documented.	**Identify the documented policies and procedures** examined to verify that the following are defined: • Development/test environments are separate from production environments with access control in place to enforce separation. • A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. • Production data (live PANs) are not used for testing or development. • Test data and accounts are removed before a production system becomes active. • Change-control procedures related to implementing security patches and software modifications are documented.	*Doc-1* *Doc-19*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.			☒	☐	☐	☐	☐
6.4.1.a Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s).	**Identify the network documentation** examined to verify that the development/test environments are separate from the production environment(s).	*Doc-1* *Doc-19* *Doc-41*					
	Describe how network device configurations verified that the development/test environments are separate from the production environment(s).	*I reviewed network device configurations in Sample Set-1 and Sample Set-2, and observed that the Office Network where testing is performed is a discrete and separate network on the FortiGate 1500D from the remainder of the network.. This allowed me to determine that the development/test environments are separate from the production environments.*					
6.4.1.b Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s).	**Identify the access control settings** examined for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	Describe how the access control settings verified that access controls are in place to enforce separation between the development/test environments and the production environment(s).	*I observed during live Zoom session production access on FortiNet firewalls and Fedora servers and found that the accounts in use do not match the temporary deployment accounts used in the test environment.*					
6.4.2 Separation of duties between development/test and production environments.			☒	☐	☐	☐	☐
6.4.2 Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment.	**Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment.	*Int-5* *Int-6*					
	Identify the personnel assigned to production environments interviewed who confirm that separation of duties is in place between development/test environments and the production environment.	*Int-5* *Int-9*					
	Describe how processes were observed to verify that separation of duties is in place between development/test environments and the production environment.	*I observed during live Zoom review with Int-7 and Int-9 that during turnup there are FortiNet devices which are staged in a testing area. I observed that during this time they are air-gapped from production. I observed that no access is possible between the networks.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			☐	☐	☒	☐	☐
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	**Identify the responsible personnel** interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	*Not Applicable. I interviewed Int-1, Int-6 and Int-9, and reviewed Doc-18 to observe that Sangoma does not develop, test, store, process or forward PAN in any form.*					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	*Not Applicable*					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	*Not Applicable*					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	**Describe how** a sample of test data was examined to verify production data (live PANs) is not used for testing.	*Not Applicable*					
	Describe how a sample of test data was examined to verify production data (live PANs) is not used for development.	*Not Applicable*					
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.			☒	☐	☐	☐	☐
6.4.4.a Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active.	**Identify the responsible personnel** interviewed who confirm that test data and accounts are removed before a production system becomes active.	*Int-5*					
	Describe how testing processes were observed to verify that test data is removed before a production system becomes active.	*I observed during live Zoom session that the turnup process is followed by Int-7 and Int-9. The process described that test accounts are not used beyond initial boot-up to change system default password. I confirmed by observation that this was the process in use.*					
	Describe how testing processes were observed to verify that test accounts are removed before a production system becomes active.	*I observed with assistance from Int-7 and Int-9 that no test accounts are used in testing beyond the initial boot-up single user account, which is changed under Doc-41 process.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.4.b Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.	**Describe how** the sampled data examined verified that test data is removed before the system becomes active.	*I observed in production Sample Set-1 and Sample Set-4 during Zoom session that no test accounts exist. I observed Int-1 attempt to log into Sample Set-4 using default accounts, and these were shown to fail as logins in production. I observed that Int-5 was unable to log into a production firewall in Sample Set-1 using the default FortiNet device default.*					
	Describe how the sampled data examined verified that test accounts are removed before the system becomes active.	*I observed in Sample Set-1 and Sample Set-4 with assistance from Int-1 and Int-5 during Zoom session that no default test accounts exist in a usable form. All defaults that remained were disabled. I read Doc-41 to confirm that the turn-up process requires that test or default accounts be changed or disabled.*					
6.4.5 Change control procedures must include the following:			☒	☐	☐	☐	☐
6.4.5.a Examine documented change-control procedures and verify procedures are defined for: • Documentation of impact. • Documented change approval by authorized parties. • Functionality testing to verify that the change does not adversely impact the security of the system. • Back-out procedures.	**Identify the documented change-control procedures** examined to verify procedures are defined for: • Documentation of impact. • Documented change approval by authorized parties. • Functionality testing to verify that the change does not adversely impact the security of the system. • Back-out procedures.	*Doc-1* *Doc-19*					
6.4.5.b For a sample of system components, interview responsible personnel to determine recent changes. Trace those changes back to related change control documentation. For each change examined, perform the following:	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-2*					
	Identify the responsible personnel interviewed to determine recent changes.	*Int-1* *Int-5*					
	For each item in the sample, **identify the sample** of changes and the related change control documentation selected for this testing procedure (through 6.4.5.4).	*Sample Set-10* *Sample Set-11*					
6.4.5.1 Documentation of impact.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.5.1 Verify that documentation of impact is included in the change control documentation for each sampled change.	*For each change from 6.4.5.b*, **describe how** the documentation of impact is included in the change control documentation for each sampled change.	*I reviewed a sample of change control screen output (Sample Set-10 and Sample Set-11) and was able to trace back each ticket by querying the change management system used by Sangoma with Int-1's assistance. I found that all tickets included a section that documented the impact of the change being requested, as is required by Doc-6 policy.*					
6.4.5.2 Documented change approval by authorized parties.			☒	☐	☐	☐	☐
6.4.5.2 Verify that documented approval by authorized parties is present for each sampled change.	*For each change from 6.4.5.b*, **describe how** documented approval by authorized parties is present in the change control documentation for each sampled change.	*I read Doc-6 and observed that it requires documentation of impact. The change control tickets that I observed in Sample Set-10 and Sample Set-11 for these vulnerability patch incidents had documentation of expected impact captured in the change control ticket.*					
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.			☒	☐	☐	☐	☐
6.4.5.3.a For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.	*For each change from 6.4.5.b*, **describe how** the change control documentation confirmed that functionality testing is performed to verify that the change does not adversely impact the security of the system.	*I read that Doc-6 requires that testing occur. The change control tickets for these vulnerability patch incidents in Sample Set-10 and Sample Set-11 included a testing notes section that is visible in the ticket dialog area. Testing includes a required security review.*					
6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	**Identify the sample** of system components selected for this testing procedure.	*Not Applicable. I determined by interview with Int-7 and review of Doc-1 that Sangoma does not develop custom code in use in any environment that it manages.*					
	For each item in the sample, **identify the sample** of custom code changes and the related change control documentation selected for this testing procedure.	*Not Applicable*					
	For each change, **describe how** the change control documentation verified that updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	*Not Applicable*					
6.4.5.4 Back-out procedures.			☒	☐	☐	☐	☐
6.4.5.4 Verify that back-out procedures are prepared for each sampled change.	*For each change from 6.4.5.b*, **describe how** the change control documentation verified that back-out procedures are prepared.	*I read Doc-19 and found that it requires that a back-out plan exist. The change control tickets (Sample Set-13) for these vulnerability patch incidents included a description of back-out as part of the plan.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.			☐	☐	☒	☐	☐
6.4.6 For a sample of significant changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	**Identify whether** a significant change occurred within the past 12 months. **(yes/no)** *If "yes," complete the following:* *If "no," mark the rest of 6.4.6 as "Not Applicable"*	*no*					
	Identify the responsible personnel interviewed for this testing procedure.	*Not Applicable*					
	Identify the relevant documentation reviewed to verify that the documentation was updated as part of the change.	*Not Applicable*					
	Identify the sample of change records examined for this testing procedure.	*Not Applicable*					
	Identify the sample of systems/networks affected by the significant change.	*Not Applicable*					
	For each sampled change, **describe how** the system/networks observed verified that applicable PCI DSS requirements were implemented and documentation updated as part of the change.						
	Not Applicable						
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. ***Note:*** *The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.5.a Examine software development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers at least annually, based on industry best practices and guidance.	**Identify the document** reviewed to verify that up-to-date training in secure coding techniques is required for developers at least annually.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	Identify the industry best practices and guidance on which the training is based.	*Not Applicable*					
6.5.b Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities	**Identify the records of training** that were examined to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities.	*Not Applicable*					
6.5.c Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities:	**Identify the software-development policies and procedures** examined to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10.	*Not Applicable*					
	Identify the responsible personnel interviewed to verify that processes are in place to protect applications from, at a minimum, the vulnerabilities from 6.5.1-6.5.10.	*Not Applicable*					
***Note:** Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external):*							
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.			☐	☐	☒	☐	☐
6.5.1 Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include: • Validating input to verify user data cannot modify meaning of commands and queries. • Utilizing parameterized queries.	*For the interviews at 6.5.c*, **summarize the relevant details** discussed to verify that injection flaws are addressed by coding techniques that include:						
	• Validating input to verify user data cannot modify meaning of commands and queries.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	• Utilizing parameterized queries.	*Not Applicable*					
6.5.2 Buffer overflow.			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.5.2 Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include: • Validating buffer boundaries. • Truncating input strings.	*For the interviews at 6.5.c*, **summarize the relevant details** discussed to verify that buffer overflows are addressed by coding techniques that include:						
	• Validating buffer boundaries.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	• Truncating input strings.	*Not Applicable*					
6.5.3 Insecure cryptographic storage.			☐	☐	☒	☐	☐
6.5.3 Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that: • Prevent cryptographic flaws. • Use strong cryptographic algorithms and keys.	*For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that insecure cryptographic storage is addressed by coding techniques that:						
	• Prevent cryptographic flaws.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	• Use strong cryptographic algorithms and keys.	*Not Applicable*					
6.5.4 Insecure communications.			☐	☐	☒	☐	☐
6.5.4 Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications.	*For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that insecure communications are addressed by coding techniques that properly:						
	• Authenticate all sensitive communications.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	• Encrypt all sensitive communications.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.5.5 Improper error handling.			☐	☐	☒	☐	☐
6.5.5 Examine software-development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details).	*For the interviews at 6.5.c*, **summarize the relevant details** discussed to verify that improper error handling is addressed by coding techniques that do not leak information via error messages.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).			☐	☐	☒	☐	☐
6.5.6 Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.	*For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
Note: *Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):*							
Indicate whether web applications and application interfaces are present. **(yes/no)** *If "no,"* mark the below 6.5.7-6.5.10 as "Not Applicable." *If "yes,"* ***complete the following:***		*no*					
6.5.7 Cross-site scripting (XSS).			☐	☐	☒	☐	☐
6.5.7 Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include: • Validating all parameters before inclusion. • Utilizing context-sensitive escaping.	*For the interviews at 6.5.c*, **summarize the relevant details** discussed to verify that cross-site scripting (XSS) is addressed by coding techniques that include:						
	• Validating all parameters before inclusion.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	• Utilizing context-sensitive escaping.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).			☐	☐	☒	☐	☐
6.5.8 Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that include: • Proper authentication of users. • Sanitizing input. • Not exposing internal object references to users. • User interfaces that do not permit access to unauthorized functions.	*For the interviews at 6.5.c*, **summarize the relevant details** discussed to verify that improper access control is addressed by coding techniques that include:						
	• Proper authentication of users.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	• Sanitizing input.	*Not Applicable*					
	• Not exposing internal object references to users.	*Not Applicable*					
	• User interfaces that do not permit access to unauthorized functions.	*Not Applicable*					
6.5.9 Cross-site request forgery (CSRF).			☐	☐	☒	☐	☐
6.5.9 Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	*For the interviews at 6.5.c*, **summarize the relevant details** discussed to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
6.5.10 Broken authentication and session management**.**			☐	☐	☒	☐	☐
6.5.10 Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include: • Flagging session tokens (for example, cookies) as "secure." • Not exposing session IDs in the URL.	*For the interviews at 6.5.c,* **summarize the relevant details** discussed to verify that broken authentication and session management are addressed via coding techniques that commonly include:						
	• Flagging session tokens (for example, cookies) as "secure."	*Not Applicable. I interviewed Int-1, Int-2 and Int-4 and determined that Sangoma does not develop custom code of any kind for its environment, and that this responsibility if it exists is the responsibility of the Sangoma customer.*					
	• Not exposing session IDs in the URL.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Incorporating appropriate time-outs and rotation of session IDs after a successful login.	• Incorporating appropriate time-outs and rotation of session IDs after a successful login.	*Not Applicable*					
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.			☐	☐	☒	☐	☐
6.6 For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows: • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security	For each public-facing web application, **identify which** of the two methods are implemented: • Web application vulnerability security assessments, AND/OR • Automated technical solution that detects and prevents web-based attacks, such as web application firewalls.	*Not Applicable. I observed by interview with Int-1 and review of firewall rules (Sample Set-1), network diagrams (Doc-42, Doc-43, Doc-44), and risk assessment document (Doc-19) to confirm that Sangoma has no public-facing web applications in use in any environment that it manages.*					
	If application vulnerability security assessments are indicated above:						
	Describe the tools and/or methods used (manual or automated, or a combination of both).	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
assessment tools or methods—as follows: – At least annually. – After any changes. – By an organization that specializes in application security. – That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. – That all vulnerabilities are corrected. – That the application is re-evaluated after the corrections. • Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: – Is situated in front of public-facing web applications to detect and prevent web-based attacks.	**Identify the documented processes** that were examined to verify that public-facing web applications are reviewed using the tools and/or methods indicated above, as follows: • At least annually. • After any changes. • By an organization that specializes in application security. • That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. • That all vulnerabilities are corrected • That the application is re-evaluated after the corrections.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
– Is actively running and up-to-date as applicable. – Is generating audit logs. – Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	**Identify the responsible personnel** interviewed who confirm that public-facing web applications are reviewed, as follows: • At least annually. • After any changes. • By an organization that specializes in application security. • That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. • That all vulnerabilities are corrected. • That the application is re-evaluated after the corrections.	*Not Applicable*					
	Identify the records of application vulnerability security assessments examined for this testing procedure.	*Not Applicable*					
	Describe how the records of application vulnerability security assessments verified that public-facing web applications are reviewed as follows:						
	• At least annually.	*Not Applicable*					
	• After any changes.	*Not Applicable*					
	• By an organization that specialized in application security.	*Not Applicable*					
	• That at a minimum, all vulnerabilities in requirement 6.5 are included in the assessment.	*Not Applicable*					
	• That all vulnerabilities are corrected.	*Not Applicable*					
	• That the application is re-evaluated after the corrections.	*Not Applicable*					
	If an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is indicated above:						
	Describe the automated technical solution in use that detects and prevents web-based attacks.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed who confirm that the above automated technical solution is in place as follows: • Is situated in front of public-facing web applications to detect and prevent web-based attacks. • Is actively running and up-to-date as applicable. • Is generating audit logs. • Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	*Not Applicable*					
	Describe how the system configuration settings verified that the above automated technical solution is in place as follows:						
	• Is situated in front of public-facing web applications to detect and prevent web-based attacks.	*Not Applicable*					
	• Is actively running and up-to-date as applicable.	*Not Applicable*					
	• Is generating audit logs.	*Not Applicable*					
	• Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	*Not Applicable*					
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
6.7 Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** examined to verify that security policies and operational procedures for developing and maintaining secure systems and applications are documented.	*Doc-1* *Doc-19*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for developing and maintaining secure systems and applications are: • In use • Known to all affected parties	*Int-1* *Int-2* *Int-4* *Int-5*					

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.			☒	☐	☐	☐	☐
7.1.a Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role. • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. • Assignment of access based on individual personnel's job classification and function. • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	**Identify the written policy for access control** that was examined to verify the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role. • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	*Doc-1* *Doc-7* *Doc-41*					
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function. • Level of privilege required (for example, user, administrator, etc.) for accessing resources.			☒	☐	☐	☐	☐
7.1.1 Select a sample of roles and verify access needs for each role are defined and include: • System components and data resources that each role needs to access for their job function.	**Identify the selected sample** of roles for this testing procedure.	*Sample Set-14* *Sample Set-15*					
	For each role in the selected sample, **describe how** the role was examined to verify access needs are defined and include:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
• Identification of privilege necessary for each role to perform their job function.	• System components and data resources that each role needs to access for their job function.	*I looked at server logins during live Zoom session in Sample Set-4 and TACACS logins for Sample Set-1, and Sample Set-2 . Members of Sample Set-14 are members of the 'wheel' group in Sample Set-4, and this enables them elevated privilege for their roles as server administrators and network engineers. I observed that members of Sample Set-15 were not members of the wheel group.*					
	• Identification of privilege necessary for each role to perform their job function.	*I read Doc-41 and observed that it identifies privileged and unprivileged users, which matches to wheel group records in Sample Set-14 and Sample Set-15. I interviewed Sample Set-14 to ask if these sampled privileges were equal to what they knew were their privileges, and they confirmed for me that this was the case. I interviewed Sample Set-15 to confirm whether their permissions matched what was defined in their TACACS and 'staff' group, and I found that the privileges they had matched those which were documented in Doc-41. I observed during live remote Zoom logins to Sample Set-4 by Sample Set-14 and Sample Set-15 and this led to a determination of compliance.*					
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.			☒	☐	☐	☐	☐
7.1.2.a Interview personnel responsible for assigning access to verify that access to privileged user IDs is: • Assigned only to roles that specifically require such privileged access. • Restricted to least privileges necessary to perform job responsibilities.	**Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is: • Assigned only to roles that specifically require such privileged access. • Restricted to least privileges necessary to perform job responsibilities.	*Int-1*					
7.1.2.b Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are: • Necessary for that individual's job function. • Restricted to least privileges necessary to perform job responsibilities.	**Identify the sample** of user IDs ***with privileged access*** selected for this testing procedure.	*Sample Set-14*					
	Identify the responsible management personnel interviewed to confirm that privileges assigned are: • Necessary for that individual's job function. • Restricted to least privileges necessary to perform job responsibilities.	*Int-1*					
	For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	• Necessary for that individual's job function.	*I interviewed Int-1 who confirmed that onboarding procedures (Doc-41) includes provisioning accounts according to the role selected, and privileged users get network access to production and test servers that unprivileged users do not receive. These follow job functions documented in Doc-1.*					
	• Restricted to least privileges necessary to perform job responsibilities.	*I interviewed Int-1 who described that users are provisioned only according to job duties.*					
7.1.3 Assign access based on individual personnel's job classification and function.			☒	☐	☐	☐	☐
7.1.3 Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual's job classification and function.	**Identify the sample** of user IDs selected for this testing procedure.	*Sample Set-14* *Sample Set-15*					
	Identify the responsible management personnel interviewed who confirm that privileges assigned are based on that individual's job classification and function.	*Int-1* *Int-2*					
	For the interview, **summarize the relevant details discussed** to confirm that privileges assigned to each sample user ID are based on that individual's job classification and function.	*I interviewed Int-1, who confirmed that policy in Doc-1 states the hiring manager must assign user privileges that are then reviewed by Int-1 (or designate) and implemented along with standard set up, confirmed by Int-3.*					
7.1.4 Require documented approval by authorized parties specifying required privileges.			☒	☐	☐	☐	☐
7.1.4 Select a sample of user IDs and compare with documented approvals to verify that: • Documented approval exists for the assigned privileges. • The approval was by authorized parties. • That specified privileges match the roles assigned to the individual.	**Identify the sample** of user IDs selected for this testing procedure.	*Sample Set-14* *Sample Set-15*					
	For each user ID in the selected sample, **describe how**:						
	• Documented approval exists for the assigned privileges.	*I looked at server record for these users as provided by Int-3's queries during live Zoom session review, and reviewed Doc-1 and Doc-7. I found that the users queried had documented approval in a column of the Turn-up procedures spreadsheet (Doc-41).*					
	• The approval was by authorized parties.	*I found in Doc-1 that every user ID was approved by Int-1, and that these are required to be given prior to creation of the accounts.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	• That specified privileges match the roles assigned to the individual.	*I asked Int-3 to query the user ID and put their privileges output (as part of their server record) on the screen. I compared this to Doc-1 and Doc-7 and found that the roles in server records matched the documented list. Int-1 confirmed that approval had been given for every role.*					
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:							
7.2 Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows:							
7.2.1 Coverage of all system components.			☒	☐	☐	☐	☐
7.2.1 Confirm that access control systems are in place on all system components.	**Identify vendor documentation** examined.	*Doc-8* *Doc-15* *Doc-21* *https://docs.fedoraproject.org/en-US/fedora/f31/system-administrators-guide/*					
	Describe how system settings and the vendor documentation verified that access control systems are in place on all system components.	*I observed Sample Set-4 with assistance from Int-3 during live Zoom session to confirm that user accounts were set up in recommended manner, and I found this was correct. Doc-47 TACACS documentation was compared to TACACS implementation. Doc-15 was reviewed to observe that user accounts and VDOM were installed as recommended by FortiNet.*					
7.2.2 Assignment of privileges to individuals based on job classification and function.			☒	☐	☐	☐	☐
7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	**Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	*I reviewed Doc-15 and reviewed Sample Set-4 with assistance from Int-4 during live Zoom session, and observed that wheel account permissions confirmed on Sample Set-4 to confirm permissions only exist for Sample Set-14. Doc-1 was reviewed and compared to Sample Set-2 and Doc-21. Privilege was assigned according to Doc-15 as confirmed in Sample Set-1.*					
7.2.3 Default "deny-all" setting.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
7.2.3 Confirm that the access control systems have a default "deny-all" setting.	**Describe how** system settings and the vendor documentation at 7.2.1 verified that access control systems have a default "deny-all" setting.	*I read Doc-1 and found that it describes process for enabling access, deny-all is standard default for users. I asked Int-3 to query a server template record, and the default had no access, and the deny-all was result. The default deny-all was recommended Palo Alto PA-3220 had definition for default no-access, and FortiNet FortiGate 1500D VDOM setting according to Doc-15 and this was observed in Sample Set-1.*					
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
7.3 Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are: • Documented, • In use, and • Known to all affected parties.	**Identify the document reviewed to** verify that security policies and operational procedures for restricting access to cardholder data are documented.	*Doc-1* *Doc-7*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for restricting access to cardholder data are: • In use • Known to all affected parties	*Int-1* *Int-3*					

Requirement 8: Identify and authenticate access to system components

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:			☒	☐	☐	☐	☐
8.1.a Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8.	**Identify the written procedures for user identification management** examined to verify processes are defined for each of the items below at 8.1.1 through 8.1.8: • Assign all users a unique ID before allowing them to access system components or cardholder data. • Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. • Immediately revoke access for any terminated users. • Remove/disable inactive user accounts at least every 90 days. • Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: – Enabled only during the time period needed and disabled when not in use. – Monitored when in use. • Limit repeated access attempts by locking out the user ID after not more than six attempts. • Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. • If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	*Doc-1* *Doc-7*				
8.1.b Verify that procedures are implemented for user identification management, by performing the following:							
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.1 Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data.	**Identify the responsible administrative personnel** interviewed who confirm that all users are assigned a unique ID for access to system components or cardholder data.	*Int-1* *Int-3*					
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.			☒	☐	☐	☐	☐
8.1.2 For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.	**Identify the sample** of privileged user IDs selected for this testing procedure.	*Sample Set-14*					
	Identify the sample of general user IDs selected for this testing procedure.	*Sample Set-15*					
	Describe how observed system settings and the associated authorizations verified that each ID has been implemented with only the privileges specified on the documented approval:						
	• For the sample of privileged user IDs.	*I looked at wheel membership for Engineers and compared membership in this to job titles listed as "privileged" in Doc-1 and found they matched.*					
	• For the sample of general user IDs.	*I looked at no accounts in the wheel group for "staff" and compared membership in this to job titles that were listed as "unprivileged" in Doc-1 and found they matched.*					
8.1.3 Immediately revoke access for any terminated users.			☒	☐	☐	☐	☐
8.1.3.a Select a sample of users terminated in the past six months, and review current user access lists—for both local and remote access—to verify that their IDs have been deactivated or removed from the access lists.	**Identify the sample** of users terminated in the past six months that were selected for this testing procedure.	*Doc-46*					
	Describe how the current user access lists for ***local access*** verified that the sampled user IDs have been deactivated or removed from the access lists.	*I reviewed Doc-46 and found that local UIDs were changed to "nologin" in Sample Set-4. I reviewed Sample Set-1 and found that accounts had been removed entirely.*					
	Describe how the current user access lists for ***remote access*** verified that the sampled user IDs have been deactivated or removed from the access lists.	*I reviewed Sample Set-1 during live Zoom session and found users were removed from the VPN entirely, which disables access because there are no local UID enabled.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.3.b Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated.	*For the sample of users terminated in the past six months at 8.1.3.a*, **describe how** it was determined which, if any, physical authentication methods, the terminated users had access to prior to termination.	*I observed with assistance from Int-10 during live Zoom session that a key fob that accesses the data center in Seattle, WA, USA was disabled by removal of name from the access list in Active Directory that can authenticate using fobs. I observed with assistance from Int-3 that the fob is retrieved from the employee, but from this point there is no access possible with the FOB even if not retrieved.*					
	Describe how the physical authentication method(s) for the terminated employees were verified to have been returned or deactivated.	*I observed with assistance from Int-10 that fobs used at data center in Seattle, WA, USA must be returned when leaving the site. I observed with assistance from Int-1 that if an employee quits, the employee account is disabled, and the fob will not work.*					
8.1.4 Remove/disable inactive user accounts within 90 days.			☒	☐	☐	☐	☐
8.1.4 Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	**Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled.	*I reviewed Doc-46 and found that no instances of users with access exceeding 90 days appeared on the list, and Int-1 explained that this was because they had been removed after 90 days.*					
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.			☐	☐	☒	☐	☐
8.1.5.a Interview personnel and observe processes for managing accounts used by third parties to access, support, or maintain system components to verify that accounts used for remote access are: • Disabled when not in use. • Enabled only when needed by the third party, and disabled when not in use.	**Identify the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are: • Disabled when not in use. • Enabled only when needed by the third party, and disabled when not in use.	*Not Applicable. I read Doc-7 and observed in the documentation that Sangoma does not by policy provide any remote access to vendors.*					
	Describe how processes for managing third party accounts were observed to verify that accounts used for remote access are:						
	• Disabled when not in use.	*Not Applicable*					
	• Enabled only when needed by the third party, and disabled when not in use.	*Not Applicable*					
8.1.5.b Interview personnel and observe processes to verify that third party remote	**Identify the responsible personnel** interviewed who confirm that accounts used by third parties for remote access are monitored while being used.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
access accounts are monitored while being used.	**Describe how** processes for managing third party remote access were observed to verify that accounts are monitored while being used.	*Not Applicable*					
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.			☒	☐	☐	☐	☐
8.1.6.a For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	For each item in the sample, **describe how** system configuration settings verified that authentication parameters are set to require that user accounts be locked after not more than six invalid logon attempts.	*I observed with assistance from Int-1 and Int-3 during connection to Administration Dashboard, that the Dashboard configuration for Administrative logins included a maximum login 5 setting. I observed with Int-1 assistance that Sample Set-4 pamd.conf settings included a maximum logins 6.*					
8.1.6.b ***Additional procedure for service provider assessments only:*** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	*Additional procedure for service provider assessments only,* **identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
	Describe how implemented processes were observed to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.			☒	☐	☐	☐	☐
8.1.7 For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	For each item in the sample, **describe how** system configuration settings verified that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	*I observed the FortiNet firewall Administration Dashboard configuration screen during live Zoom session for the password rules on the Sangoma administrative panel shown by Int-1 in Sample Set-1. I observed pamd.conf configuration setting in Sample Set-4 shown to me by Int-1 was set to lockout=30 (minutes).*					
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.1.8 For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	For each item in the sample, **describe how** system configuration settings verified that system/session idle time out features have been set to 15 minutes or less.	*I asked for and was shown FortiNet Administrative Dashboard by Int-1 and found that session idle time out was set to 15 minutes. I reviewed with Int-1 assistance the pamd.conf variables in Sample Set-4 and found that these were idle timeout set to 5 minutes.*					
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric.			☒	☐	☐	☐	☐
8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following: • Examine documentation describing the authentication method(s) used. • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	**Identify the document** describing the authentication method(s) used that was reviewed to verify that the methods require users to be authenticated using a unique ID and additional authentication for access to the cardholder data environment.	*Doc-6* *Doc-7*					
	Describe the authentication methods used (for example, a password or passphrase, a token device or smart card, a biometric, etc.) for each type of system component.	*I observed during live Zoom session with assistance from Int-1 that Sangoma is using strong passwords and two-factor authentication for access to the Jump servers in Sample Set-8. I learned from Int-1 by interview and by review of Sample Set-1 and Sample Set-2 that remote access must be performed using Sample Set-8.*					
	For each type of authentication method used and for each type of system component, **describe how** the authentication method was observed to be functioning consistently with the documented authentication method(s).	*I observed FortiGate FortiClient access in use for every login session to servers in Sample Set-4 in the managed Sangoma environment. I observed that the Google authenticator plug-in is used to send the second factor to employees' smart phones. Int-1 showed me the authentication sequence by using the camera on the notebook to show off google authenticator in operation during the login sessions I observed by live Zoom session.*					
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.1.a Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage.	**Identify the vendor documentation** examined to verify that passwords are protected with strong cryptography during transmission and storage.	*Doc-15*					
	Identify the sample of system components selected for this testing procedure.	*Sample Set-1*					
	For each item in the sample, **describe how** system configuration settings verified that passwords are protected with strong cryptography during ***transmission***.	*I observed during live Zoom session that the login sessions that used the FortiNet VPN and two-factor authentication. I saw browser tab for show-certificate and saw the certificate in all sessions reviewed. The VPN session did not function without the cryptography certificate being accepted.* *I observed during live Zoom session that the logins that used the Palo Alto devices were required to go through a jump station (Sample Set-8) which used two factor (Google Authenticator) authentication in the server's pamd.conf file which set AES 256-bit / RSA 2048-bit and used google certificates, which was then, connected to Sangoma's TACACS+ authentication configuration (Sample Set-5)*					
	For each item in the sample, **describe how** system configuration settings verified that passwords are protected with strong cryptography during ***storage***.	*I observed in the clients shown to me by Sample Set-14 logins contained, FortiClient TLS v1.2 AES 256-bit / RSA 2048-bit certificate* *I observed in the TACACS+ configuration that jump server sessions were using AES 256-bit / RSA 2048-bit certificates, shown in the configuration (pamd.conf) on the servers (Sample Set-8)*					
8.2.1.b For a sample of system components, examine password files to verify that passwords are unreadable during storage.	*For each item in the sample at 8.2.1.a,* **describe how** password files verified that passwords are unreadable during storage.	*I observed sample client configuration files (Sample Set-19) and found that password file storage was encrypted using AES 256-bit.*					
8.2.1.c For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission.	*For each item in the sample at 8.2.1.a,* **describe how** data transmissions verified that passwords are unreadable during transmission.	*I observed FortiNet VPN login sessions and found they all used the certificate provided to log in, the browser showed the locked icon and https was the protocol being used.* *I observed in sessions to Palo Alto that were required to authenticate through jump servers (Sample Set-8) that SSH v2 was the protocol used, observed in the pamd.conf configuration file.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.1.d ***Additional procedure for service provider assessments only:*** Observe password files to verify that non-consumer customer passwords are unreadable during storage.	*Additional procedure for service provider assessments only: for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during storage.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
8.2.1.e ***Additional procedure for service provider assessments only:*** Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission.	*Additional procedure for service provider assessments only: for each item in the sample at 8.2.1.a,* **describe how** password files verified that non-consumer customer passwords are unreadable during transmission.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.			☒	☐	☐	☐	☐
8.2.2 Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the authentication credential is modified.	**Identify the document** examined to verify that authentication procedures for modifying authentication credentials define that if a user requests a reset of an authentication credential by a non-face-to-face method, the user's identity is verified before the authentication credential is modified.	*Doc-7*					
	Describe the non-face-to-face methods used for requesting password resets.	*I observed in Doc-7 that employees are required to have password reset confirmed by approval of Security team, or managerial approval if this is not available.*					
	For each non-face-to-face method, **describe how** security personnel were observed to verify the user's identity before the authentication credential was modified.	*I observed from Doc-7 document that support requests made must be approved by a manager or security approver.*					
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.3.a For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	For each item in the sample, **describe how** system configuration settings verified that user password/passphrase parameters are set to require at least the following strength/complexity:						
	• Require a minimum length of at least seven characters.	*I observed during live Zoom session that password rules are set globally. The configuration captured shows minimum length set to 8 characters. This was shown by the Sample Set-4 snapshot of server password store authoritative for Sangoma administrators. For FortiNet VPN users, password policies are set by FortiGate policy as seen in Sample Set-1.*					
	• Contain both numeric and alphabetic characters.	*I observed in Sample Set-4 during live remote Zoom session that password store rules include the following:* ▪ *Minimum required digit characters: 1* ▪ *Minimum required alpha characters: 1* ▪ *Minimum required uppercase characters: 1* ▪ *Minimum required lowercase characters: 1* ▪ *Minimum required special characters: 1* ▪ *Minimum required character categories: 3* *Thus, a password is required to have 3 elements of complexity chosen from this list and is above the PCI requirement for numeric and alphabetic.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.3.b ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	*Additional procedure for service provider assessments only:* **Identify the documented internal processes and customer/user documentation** reviewed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: • A minimum length of at least seven characters. • Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
	Describe how internal processes were observed to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:						
	• A minimum length of at least seven characters.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
	• Non-consumer customer passwords/passphrases are required to contain both numeric and alphabetic characters.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
8.2.4 Change user passwords/passphrases at least once every 90 days.			☒	☐	☐	☐	☐
8.2.4.a For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	For each item in the sample, **describe how** system configuration settings verified that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days.	*I asked to see the FortiNet password settings in Sample Set-1 and observed that they require a password change within 90 days. I asked to see the pamd.conf password rules in Sample Set-4 and observed the password history configuration was set to 90 days.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.2.4.b ***Additional procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that: • Non-consumer customer user passwords/passphrases are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	*Additional procedure for service provider assessments only,* **identify the documented internal processes and customer/user documentation** reviewed to verify that: • Non-consumer customer user passwords/passphrases are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
	Describe how internal processes were observed to verify that:						
	• Non-consumer customer user passwords/passphrases are required to change periodically; and	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
	• Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.			☒	☐	☐	☐	☐
8.2.5.a For a sample of system components, obtain and inspect system configuration settings to verify that password/passphrase parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	For each item in the sample, **describe how** system configuration settings verified that password/passphrase parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	*In Sample Set-1 I observed with assistance from Int-1 during live Zoom session that FortiGate password history is set to 4. In Sample Set-4 I observed with assistance from Int-1 that the servers pamd.conf files in all cases was history 4, which required four previous passwords to be unique.*					
8.2.5.b ***Additional Procedure for service provider assessments only:*** Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrases cannot be the	*Additional procedure for service provider assessments only,* **identify the documented internal processes and customer/user documentation** reviewed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
same as the previous four passwords/passphrases.	**Describe how** internal processes were observed to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases.	*Not Applicable. I reviewed Doc-7 and interviewed Int-1 to confirm that while Sangoma is a service provider, it provides no non-consumer customer passwords to its customers.*					
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.			☒	☐	☐	☐	☐
8.2.6 Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use.	**Identify the documented password procedures** examined to verify the procedures define that: • First-time passwords/passphrases must be set to a unique value for each user. • First-time passwords/passphrases must be changed after the first use. • Reset passwords/passphrases must be set to a unique value for each user. • Reset passwords/passphrases must be changed after the first use.	*Doc-7*					
	Describe how security personnel were observed to:						
	• Set first-time passwords/passphrases to a unique value for each new user.	*I observed a password creation process undertaken at Sangoma in which int-3 generated new accounts. The new accounts (2) were required to be created using unique passwords.*					
	• Set first-time passwords/passphrases to be changed after first use.	*I observed password creation by Int-3 at Sangoma. The new account was logged into and prompted to change the initial password upon initial login.*					
	• Set reset passwords/passphrases to a unique value for each existing user.	*I observed two password reset demonstrations by Int-3 at Sangoma. The passwords reset was not allowed to be set to a copied default value. A unique password only was allowed.*					
	• Set reset passwords/passphrases to be changed after first use.	*I then observed these accounts passwords be logged into, and both were required to change the password that had just been reset after the first reset use.*					
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*							

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.			☒	☐	☐	☐	☐
8.3.1.a Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE.	**Identify the sample of network and/or system components** examined for this testing procedure.	*Sample Set-1* *Sample Set-4*					
	Describe how the configurations verify that multi-factor authentication is required for all non-console access into the CDE.						
	I observed live remote Sample Set-14 log into FortiGate client and use a second factor sent to their phones. I observed the access is required to be sent to google authenticator in the LDAP and PAM files I observed this action matched the configuration screen I was shown, and this led to a determination of compliance..						
8.3.1.b Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used.	**Identify the sample of administrator personnel** observed logging in to the CDE.	*Sample Set-14*					
	Describe the multi-factor authentication methods observed to be in place for administrator personnel non-console log ins to the CDE.						
	I observed live remote Sample Set-14 log into FortiGate client and use a second factor sent to their phones using the google two-factor process. Sample Set-15 is not granted remote VPN access to the servers and had no two-factor process.						
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.			☒	☐	☐	☐	☐
8.3.2.a Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for: • All remote access by personnel, both user and administrator, and • All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes).	**Describe how** system configurations for remote access servers and systems verified that multi-factor authentication is required for:						
	• All remote access by personnel, both user and administrator, and	*I observed live remote in Sample Set-15 that remote multi-factor access is not enabled at all. I observed in Sample Set-14 that google account must be configured to send multi-factor authentication to their smart phone prior to the login being accepted.*					
	• All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes).	*Not Applicable. Third parties/vendors are not allowed remote access by Sangoma policy as documented in Doc-7.*					
8.3.2.b Observe a sample of personnel (for example, users and administrators)	**Identify the sample of personnel** observed connecting remotely to the network.	*Sample Set-14*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
connecting remotely to the network and verify that at least two of the three authentication methods are used.	*For each individual in the sample,* **describe how** multi-factor authentication was observed to be required for remote access to the network.	*I observed during live remote Zoom demonstration the multi-factor process as follows: Something they needed to know was the administrative login password. The "something they knew" was the administrative account in their possession. The "something they had" was the smart phone provisioned with the google app configured to receive the second factor needed for the login to complete successfully.*					
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials. • Guidance for how users should protect their authentication credentials. • Instructions not to reuse previously used passwords. • Instructions to change passwords if there is any suspicion the password could be compromised.			☒	☐	☐	☐	☐
8.4.a Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users.	**Identify the documented policies and procedures** examined to verify authentication procedures define that authentication procedures and policies are distributed to all users.	*Doc-1* *Doc-7*					
	Identify the responsible personnel interviewed who confirm that authentication policies and procedures are distributed to all users.	*Int-1*					
8.4.b Review authentication policies and procedures that are distributed to users and verify they include: • Guidance on selecting strong authentication credentials. • Guidance for how users should protect their authentication credentials. • Instructions for users not to reuse previously used passwords. • Instructions to change passwords if there is any suspicion the password could be compromised.	**Identify the documented authentication policies and procedures that are distributed to users** reviewed to verify they include: • Guidance on selecting strong authentication credentials. • Guidance for how users should protect their authentication credentials. • Instructions for users not to reuse previously used passwords. • That users should change passwords if there is any suspicion the password could be compromised.	*Doc-7*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.4.c Interview a sample of users to verify that they are familiar with authentication policies and procedures.	**Identify the sample** of users interviewed for this testing procedure.	*Sample Set-14* *Sample Set-15*					
	For each user in the sample, **summarize the relevant details** discussed that verify that they are familiar with authentication policies and procedures.	*I observed that the Engineering users (privileged) in Sample Set-14 were aware of two-factor use and remote access to the administrative environment. All interviewees are familiar with password reset procedure, password strength, and password procedures. I observed that Sample Set-15 were provided no remote administrative access.*					
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.			☒	☐	☐	☐	☐
8.5.a For a sample of system components, examine user ID lists to verify the following: • Generic user IDs are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used to administer any system components.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-4*					
	For each item in the sample, **describe how** the user ID lists verified that:						
	• Generic user IDs are disabled or removed.	*I reviewed a sanitized /etc/shadow provided in sample of servers from Sample Set-4 during live Zoom session. Generic user ID were marked as disabled using the asterisk character in the password field, and shell accounts were set to /bin/false. These details indicate that the accounts are disabled, and cannot be used to log in.*					
	• Shared user IDs for system administration activities and other critical functions do not exist.	*I observed in Sample Set-4 that none of the shared accounts that were marked with an asterisk are used by Sangoma for any functions.*					
	• Shared and generic user IDs are not used to administer any system components.	*None of the shared or generic accounts are used by Sangoma to administer any system attributes. The only accounts which allow remote login are the users' own account, plus using the 'sudo' command to perform elevated privilege commands when appropriate.*					
8.5.b Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.	**Identify the documented policies and procedures** examined to verify authentication policies/procedures define that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.	*Doc-1* *Doc-14*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.5.c Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.	**Identify the system administrators** interviewed who confirm that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.	*Int-1* *Int-2*					
8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*			☐	☐	☒	☐	☐
8.5.1 ***Additional procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer.	**Identify the documented procedures** examined to verify that different authentication credentials are used for access to each customer.	*Not Applicable. I reviewed Doc-14 and interviewed Int-1 to confirm that while Sangoma is a service provider, there are no POS systems in use, nor servers in use for customers that Sangoma supports.*					
	Identify the responsible personnel interviewed who confirm that different authentication credentials are used for access to each customer	*Not Applicable*					
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.			☒	☐	☐	☐	☐
8.6.a Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include: • Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.	**Identify the documented authentication policies and procedures** examined to verify the procedures for using authentication mechanisms define that: • Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.	*Doc-1* *Doc-7*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.6.b Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts.	**Identify the security personnel** interviewed who confirm that authentication mechanisms are assigned to an account and not shared among multiple accounts.	*Int-1*					
8.6.c Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access.	**Identify the sample** of system components selected for this testing procedure.	*Sample Set-4*					
	For each item in the sample, **describe how** system configuration settings and/or physical controls, as applicable, verified that controls are implemented to ensure only the intended account can use that mechanism to gain access.	*During live log-in sessions conducted by Int-1 during live remote Zoom interviews, I had the administrator export the IP tables to the screen and share it. These IP tables were then observed visually, and I asked Int-1 to explain the configurations seen. Int-1 described that IP tables configuration in Sample Set-4 are locked down to only the trusted server IP being able to be connected to by the authorized administrative IP.*					
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).			☐	☐	☒	☐	☐
8.7.a Review database and application configuration settings and verify that all users are authenticated prior to access.	**Identify** all databases containing cardholder data.	*Not Applicable. I validated by interview with Int-1 and live display of sample data provided by Int-3 of Sample Set-1 and Sample Set-4 that Sangoma has no databases that contain cardholder data.*					
	Describe how database and/or application configuration settings verified that all users are authenticated prior to access.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
8.7.b Examine database and application configuration settings to verify that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).	*For each database from 8.7.a,* **describe how** the database and application configuration settings verified that all user access to, user queries of, and user actions on the database are through programmatic methods only.	*Not Applicable*					
8.7.c Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators.	*For each database from 8.7.a*, **describe how** database application configuration settings verified that user direct access to or queries of databases are restricted to database administrators.	*Not Applicable*					
8.7.d Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).	*For each database from 8.7.a:*						
	Identify applications with access to the database.	*Not Applicable*					
	Describe how database access control settings, database application configuration settings and related application IDs verified that application IDs can only be used by the applications.	*Not Applicable*					
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
8.8 Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for identification and authentication are documented.	*Doc-1* *Doc-7*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for identification and authentication are: • In use • Known to all affected parties	*Int-1* *Int-3*					

Requirement 9: Restrict physical access to cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.			☒	☐	☐	☐	☐
9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas	**Identify and briefly describe** all of the following with systems in the cardholder data environment:						
	• All computer rooms	*Not Applicable. I interviewed Int-1 and reviewed Doc-14 to find that there are no computer rooms in the Sangoma network that contain CHD.*					

with systems in the cardholder data environment. • Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. • Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder data environment and verify that they are "locked" to prevent unauthorized use.	• All data centers	*I observed by on-site personnel at the Seattle, WA, USA and by remote Zoom at the Los Angeles, CA, USA data centers that the following controls were in place:* • *Guard on duty 24/7* • *Man trap* • *Smart card reader* • *Cameras at entrance points and sensitive zones* *I reviewed Doc-14 and found that the responsibilities for these requirements for physical security including guard on duty, man-trap, smart-card reader and cameras were those of the data center service providers in use by Sangoma:* *I read the AoCs for these data centers provided to me by Sangoma (Doc-9, Doc-22, Doc-45) and found that the data centers were PCI-DSS v3.2.1 approved service providers for these requirements.* *Digital Realty Data Center, New York, NY, USA (in scope, AoC, v3.2.1, 28 Feb 2023)* *Digital Realty Data Center, Atlanta, GA, USA (in scope, AoC, v3.2.1, 28 Feb 2023)* *Digital Realty Data Center, Dallas, TX, USA (in scope, AoC, v3.2.1, 28 Feb 2023)* *CoreSite Data Center, Denver, CO, USA (in scope, AoC, v3.2.1, 30 Jun 2023)* *Equinix Data Center, Chicago, IL, USA (in scope, AoC, v3.2,1, 5 Nov 2023)* *CoreSite Data Center, San Jose, CA, USA (in scope, AoC, v3.2.1, 30 Jun 2023)* *Digital Realty Data Center, San Francisco, CA, USA (in scope, AoC, v3.2.1, 28 Feb 2023)* *Digital Realty Data Center, Marseilles, FR (in scope, AoC, v3.2.1, 28 Feb 2023)* *Digital Realty Data Center, Johannesburg, South Africa (in scope, AoC v3.2.1, 28 Feb 2023)* *Equinix Data Center, Toronto, ON, Canada (in scope, AoC, v3.2.1, 5 Nov 2023)* *CoreSite Data Center, Reston, VA, USA (in scope, AoC, v3.2.1, 30 Jun 2023)*

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
		CoreSite Data Center, Los Angeles, CA, USA (in scope, AOC, v3.2.1, 30 Jun 2023) *Equinix Data Center, Sydney, NSW, Australia (in scope, AoC, v3.2.1, 5 Nov 2023)*					
	• Any other physical areas	*Not Applicable. I interviewed Int-1 and reviewed Doc-14 to find that there are no other physical areas in the Sangoma network that contain CHD.*					
	For each area identified (add rows as needed), complete the following:						

	Describe the physical security controls observed to be in place, including authorized badges and lock and key.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed at Lunavi that badges were used by all employees. I observed that photographs of employees existed on badges. I observed that I was given a blank visitor badge in exchange for my government ID (Drivers' license). The visitor badge had no photograph. Badges were kept behind secure glass managed by Digital Realty employee on the first floor of the facility where we checked in. The badge was required to be returned by me to have my government ID (drivers' license) returned prior to departure. This led to a determination of compliance.*

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	Identify the randomly selected systems in the cardholder environment for which a system administrator login attempt was observed.	*Sample Set-1* *Sample Set-4* *Sample Set-9*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	Describe how consoles for the randomly selected systems were observed to be "locked" when not in use.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed in person with assistance from Int-3 and Int-10 that Sangoma cabinets were locked in the data center managed by Lunavi. My attempt to open the cabinets failed when tried.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.1.a Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas.	**Describe** either the video cameras or access control mechanisms (or both) observed to monitor the entry/exit points to sensitive areas.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed in person with assistance from Int-10 and Int-3 that there were video camera positioned on the aisles next to Sangoma equipment in the Lunavi facility, as well as next to the exit doors to the floor.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.1.b Verify that either video cameras or access control mechanisms (or both) are protected from tampering or disabling.	**Describe how** either the video cameras or access control mechanisms (or both) were observed to be protected from tampering and/or disabling.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility. I observed recessed bolt mounts to ceilings for the cameras, as well as dome-shaped protective covers. I observed that tampering with these was protected. Int-10 also described that attempts to tamper with would be seen by on-staff monitoring of the cameras due to the motion involved.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.1.c Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months.	**Describe how** the data from video cameras and/or access control mechanisms were observed to be reviewed.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed with assistance from Int-10 that the cameras for Lunavi were monitored from their office on a separate floor at the Seattle, WA, USA facility. Int-10 was able to show me the floor and cabinet where I visited with Int-3's assistance. Int-10 said that these cameras were being observed 24/7/365.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	Describe how data was observed to be stored for at least three months.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I asked Int-10 to produce camera images for the Sangoma site inside Lunavi facility for 90 days ago, and Int-10 was able to produce these images. This led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.2 Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks.	**Identify the responsible personnel** interviewed who confirm that physical and/or logical controls are in place to restrict access to publicly accessible network jacks.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed during site visit to Lunavi facility in Seattle, WA, USA that no network jacks were available at all in any public areas. This led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	Describe how physical and/or logical controls were observed to be in place to restrict access to publicly accessible network jacks.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed with assistance from Int-3 and Int-10 that no network jacks were available in the public waiting area or any other corridor or public-facing area at the Lunavi facility at Seattle, WA, USA. This led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	Describe how physical access was observed to be restricted to the following:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.1.3 Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.	• Wireless access points	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed that "Guest Wi-Fi" was available in the lobby of the facility. I asked Int-10 whether this wi-fi granted any access to Lunavi or Sangoma networking, and he confirmed for me that it did not. I asked Int-3 whether there was a Wi-fi access point in use for Sangoma at this facility, and he said there was not. This led to a determination of compliance.*					

	• Wireless gateways	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed that "Guest Wi-Fi" was available in the lobby of the facility. I asked Int-10 whether this wi-fi granted any access to Lunavi or Sangoma networking, and he confirmed for me that it did not. I asked whether Lunavi operates a wi-fi gateway, and was told that it does not. I asked Int-3 whether there was a Wi-fi access point in use for Sangoma at this facility, and he said there was not. This led to a determination of compliance.*
	• Wireless handheld devices	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for*

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
		Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity. *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *Int-10 confirmed for me that Lunavi does not use handheld wi-fi devices to access its networks at this facility. This led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	• Network/communications hardware	*I confirmed by in-person interview with Int-10 at the Seattle, WA, USA facility that Sangoma has network/communications hardware locked in limited-access closet. There is a physical key required, which is under strict distribution to managers only. I observed in Sample Set-18 sites shown to me that no customer or guest access exists to network and communications hardware.* *I read Doc-30 and found that this responsibility was tracked as being the responsibility of the data centers in Sample Set-16.* *I read the Digital Realty AoC (v3.2.1, 28 Feb 2023) and observed that this requirement was their responsibility for Sangoma data centers in New York, NY, USA; Atlanta, GA, USA, Dallas, TX, USA; San Francisco, CA, USA; Johannesburg, South Africa; and Marseilles, FR.* *I read the CoreSite AoC (v3.2.1, 30 Jun 2023) and observed that this requirement was their responsibility for Sangoma data centers in Denver, CO, USA; San Jose, CA, USA; Los Angeles, CA, USA; Reston, VA, USA.* *I read the Equinix AoC (v3.2.1, 5 Nov 2023) and observed that this requirement was their responsibility for Sangoma in Chicago, IL, USA; Toronto, ON, Canada; Sydney, NSW, Australia*					
	• Telecommunication lines	*I reviewed Attestations of Compliance (AoC) to confirm that Sample Set-16 has this requirement met for Sangoma.*					
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges). • Changes to access requirements. • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.2.a Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors. Verify procedures include the following: • Identifying onsite personnel and visitors (for example, assigning badges), • Changing access requirements, and • Revoking terminated onsite personnel and expired visitor identification (such as ID badges).	**Identify the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following: • Identifying onsite personnel and visitors (for example, assigning badges), • Changing access requirements, and • Revoking terminated onsite personnel and expired visitor identification (such as ID badges).	*Doc-7*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.2.b Examine identification methods (such as ID badges) and observe processes for identifying and distinguishing between onsite personnel and visitors to verify that: • Visitors are clearly identified, and • It is easy to distinguish between onsite personnel and visitors.	**Identify** the identification methods examined.	*I verified this is the responsibility of Service Provider CoreSite in facilities in Atlanta, GA, USA; Chicago, IL, USA; Reston, VA, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; Clifton, NJ, USA; San Francisco, CA, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 30 Jun 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed ID badges with photos on them in use at the Lunavi facility at Seattle, WA, USA. I observed that the guest visitor badge I was given contained no photograph. I observed with assistance from Int-10 that I was required to wear the visitor badge around my neck/attached to my shirt at all times in the facility. This led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	Describe how processes for identifying and distinguishing between onsite personnel and visitors were observed to verify that:						
	• Visitors are clearly identified, and	*I read Doc-30 and found that this responsibility was tracked as being the responsibility of the data centers.* *I read the Digital Realty AoC (v3.2.1, 28 Feb 2023) and observed that this requirement was their responsibility for Sangoma data centers in New York, NY, Clifton, NJ, USA; Atlanta, GA, USA, Dallas, TX, USA; San Francisco, CA, USA; Johannesburg, South Africa; Marseilles, FR.* *I read the CoreSite AoC (v3.2.1, 30 Jun 2023) and observed that this requirement was their responsibility for Sangoma data centers in Atlanta, GA, USA; Denver, CO, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA.* *I read the Equinix AoC (v3.2.1, 5 Nov 2023) and observed that this requirement was their responsibility for Sangoma in Chicago, IL, USA; Toronto, ON, Canada; Sydney, NSW, Australia.* *I observed by live visit with assistance from Int-10 on-site at Lunavi data center in Seattle, WA, USA that this requirement was met by the building issuing sticker ID to all visitors, with no company logo and an expiration date visible. This differed from employee ID which all contained company logos.*					

	• It is easy to distinguish between onsite personnel and visitors.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I validated the compliance of these PCI-DSS v3.2.1 requirements of Lunavi by live site visit with Int-3 and on-site interview with Int-10, following a live-walkaround to observe camera positions, data center sign-in, doorway multi-factor authentication, badging, sign-in and out, exit door position and camera, Sangoma equipment row and camera, position of data destruction and any consoles, wall jacks and cage boundaries, to observe that Lunavi is compliant with these requirements.*
9.2.c Verify that access to the identification process (such as a badge	**Describe how** access to the identification process was observed to be limited to authorized personnel.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service*

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
system) is limited to authorized personnel.		*provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I validated the compliance of these PCI-DSS v3.2.1 requirements of Lunavi by live site visit with Int-3 and on-site interview with Int-10, following a live-walkaround script and live instructions given, to doorway multi-factor authentication and badging. This led to a determination of compliance.*					
9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.3.a For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that: • Access to the sensitive area is authorized. • Access is required for the individual's job function.	**Identify the sample** of responsible personnel interviewed for this testing procedure.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I validated the compliance of these PCI-DSS v3.2.1 requirements of Lunavi by live site visit with Int-3 and on-site interview with Int-10. I observed that badge and thumb scan were required to enter the protected data center room. Int-10 showed me the management of authorized employees on his workstation screen in his office. This list showed Sangoma authorized employees (Int-3 among them) and led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	For the interview, **summarize the relevant details** discussed to verify that:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	• Access to the sensitive area is authorized.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *Int-10 told me that to gain access to this list, Lunavi requires that the person is validated as an employee of the customer company, in this case Sangoma. Int-3 confirmed for me he had to be verified by Lunavi to add anybody to be granted site access. The use of this procedure led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
	• Access is required for the individual's job function.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I asked Int-10 if anyone can get access to the facility's authorized list and be added to electronic access. He told me only employees of Sangoma are allowed. Int-3 confirmed this for me, and this led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.3.b Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access.	**Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I was told by Int-10 that every 90 days, they contact the number on file provided to them by Sangoma and confirm if access is still required. Int-3 confirmed this for me. This led to a determination of compliance that all access must be granted only to authorized personnel at Sangoma.*					
	Identify the sample of users recently terminated.	*Doc-46*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.3.c Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas.	*For all items in the sample,* **provide the name of the assessor** who attests that the access control lists were reviewed to verify the personnel do not have physical access to sensitive areas.	*David M Dennis*					
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:							
9.4 Verify that visitor authorization and access controls are in place as follows:							
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.			☒	☐	☐	☐	☐
9.4.1.a Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.	**Identify the documented procedures** examined to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.	*Doc-7*					
	Identify the responsible personnel interviewed who confirm that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.	*Int-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.4.1.b Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained.	**Describe how** the use of visitor badges or other identification was observed to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed that it is impossible for unauthorized personnel to get past the first floor lobby at the Lunavi facility unless they are escorted. The elevator in use will not move past the floor unless staff enable it to proceed. Int-10 confirmed this is the process used for all visitors. This led to a determination of compliance.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.			☒	☐	☐	☐	☐
9.4.2.a Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel.	**Describe how** people within the facility were observed to use visitor badges or other identification.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed with assistance from Int-10 and Int-3 that my visitor badge was different than the visitor badge granted to authorized guest (Int-3) or on-site employee (Int-10). This led to a determination of compliance.*					

	Describe how visitors within the facility were observed to be easily distinguishable from onsite personnel.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I validated the compliance of these PCI-DSS v3.2.1 requirements of Lunavi by live remote Zoom site visit with Int-1 and on-site interview with Int-10, following a live-walkaround script and live instructions given, to observe camera positions, data center sign-in, doorway multi-factor authentication, badging, sign-in and out, exit door position and camera, Sangoma equipment row and camera, position of data destruction and any consoles, wall jacks and cage boundaries, to observe that Lunavi is compliant with these requirements.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Los Angeles, CA, USA facility.*

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
		I observed employee and facility badges were in use at Lunavi at the Seattle, WA, USA facility. This was easily distinguishable from guest visitor badges. This led to a determination of compliance.					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.4.2.b Verify that visitor badges or other identification expire.	**Describe how** visitor badges or other identification were verified to expire.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed that my guest visitor badge granted no access, and there was nothing to "expire." I observed that my authorization to be on the facility expired in 2 hrs, according to Int-10. This led to a determination of compliance.*					
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.4.3 Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration.	**Describe how** visitors leaving the facility were observed to verify they are asked to surrender their badge or other identification upon departure or expiration.	*I verified this is the responsibility of Service Provider CoreSite in facilities in San Jose, CA, USA; Reston, VA, USA; Chicago, IL, USA; Los Angeles, CA, USA; and Denver, CO, USA, as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider CoreSite, dated 30 Jun 2023 (Doc-22), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Digital Realty in facilities in Atlanta, GA, USA; Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Marseilles, FR; Johannesburg, South Africa; New York, NY, USA; as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Digital Realty, dated 28 Feb 2023 (Doc-45), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I verified this is the responsibility of Service Provider Equinix in facilities in Chicago, IL, USA; Sydney, NSW, Australia Toronto, ON, Canada as verified through review of Sangoma service provider tracker tab (Doc-14) and responsibility matrix (Doc-30). I reviewed the AOC for Service Provider Equinix, dated 5 Nov 2023 (Doc-9), and confirmed the service provider was found to be PCI DSS compliant against PCI DSS v3.2.1 for all applicable requirements, and that it covers the scope of the services used by the assessed entity.* *I read Doc-30 to confirm requirements provided by Lunavi, and which are provided by Sangoma in the Seattle, WA, USA facility.* *I observed that my guest visitor badge was required to be surrendered upon my departure from the facility, in order for me to have my government ID (drivers' license) returned to me. As a result, I could not keep the badge.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.			☒	☐	☐	☐	☐
9.4.4.a Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.	**Describe how** it was observed that a visitor log is in use to record physical access to:						
	• The facility	*I read the Digital Realty AoC (v3.2.1, 28 Feb 2023) and observed that this requirement was their responsibility for Sangoma data centers in New York, NY, USA; Atlanta, GA, USA, Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Johannesburg, South Africa; Marseilles, FR.* *I read the CoreSite AoC (v3.2.1, 30 Jun 2023) and observed that this requirement was their responsibility for Sangoma data centers in Denver, CO, USA; Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA.* *I read the Equinix AoC (v3.2.1, 5 Nov 2023) and observed that this requirement was their responsibility for Sangoma in Chicago, IL, USA; Toronto, ON, Canada; Sydney, NSW, Australia.* *I observed by in-person session with assistance from Int-10 at Lunavi data center in Seattle, WA, USA that this requirement was met by logs used by the facility security guard used to log to all visitors.*					
	• Computer rooms and data centers where cardholder data is stored or transmitted.	*Not Applicable. I interviewed Int-1 and Int-2 and reviewed Doc-19 to learn that Sangoma does not store, process or transmit cardholder data.*					
9.4.4.b Verify that the log contains: • The visitor's name, • The firm represented, and • The onsite personnel authorizing physical access.	**Provide the name of the assessor** who attests that the visitor log contains: • The visitor's name, • The firm represented, and • The onsite personnel authorizing physical access.	*David M Dennis*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.4.4.c Verify that the log is retained for at least three months.	**Describe how** visitor logs were observed to be retained for at least three months.	*I read the Digital Realty AoC (v3.2.1, 28 Feb 2023) and observed that this requirement was their responsibility for Sangoma data centers in New York, NY, USA; Atlanta, GA, USA, Dallas, TX, USA; San Francisco, CA, USA; Clifton, NJ, USA; Johannesburg, South Africa; Marseilles, FR.* *I read the CoreSite AoC (v3.2.1, 30 Jun 2023) and observed that this requirement was their responsibility for Sangoma data centers in Denver, CO, USA; Atlanta, GA, USA; Chicago, IL, USA; Los Angeles, CA, USA; Reston, VA, USA.* *I read the Equinix AoC (v3.2.1, 5 Nov 2023) and observed that this requirement was their responsibility for Sangoma in Chicago, IL, USA; Toronto, ON, Canada; Sydney, NSW, Australia.* *I observed with assistance from Int-10 at Lunavi data center in Seattle, WA, USA that this requirement was met by visitor ID being retained on side. I asked to see and was shown old log sheets with dates over 90 days ago.*					
9.5 Physically secure all media.			☒	☐	☐	☐	☐
9.5 Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).	**Identify the documented procedures for protecting cardholder data** reviewed to verify controls for physically securing all media are defined.	*I read Doc-14 and reviewed Doc-7 to validate this control was in place provided by Sample Set-16.*					
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.			☐	☐	☒	☐	☐
9.5.1 Verify that the storage location security is reviewed at least annually to confirm that backup media storage is secure.	**Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure.	*Not Applicable. Sangoma has no cardholder data stored in any of its collocated data center facilities, as confirmed by site-visit as well as by interview with Int-1*					
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.6 Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.	**Identify the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals.	*Not Applicable. Sangoma under Doc-1 and Doc-3 has no media which contains CHD stored, nor any CHD on paper media, in its environment.*					
9.6.1 Classify media so the sensitivity of the data can be determined.			☐	☐	☒	☐	☐
9.6.1 Verify that all media is classified so the sensitivity of the data can be determined.	**Describe how** media was observed to be classified so the sensitivity of the data can be determined.	*Not Applicable. I read Doc-7 and Doc-14 to find that any co-located data center media is the responsibility of Sample Set-16.*					
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.			☐	☐	☒	☐	☐
9.6.2.a Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.	**Identify the responsible personnel** interviewed who confirm that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.	*Not Applicable. Sangoma under Doc-1 and Doc-3 has no media which contains CHD stored, nor any CHD on paper media, in its environment.*					
	Identify the records examined for this testing procedure.	*Not Applicable*					
	Describe how the offsite tracking records verified that all media is logged and sent via secured courier or other delivery method that can be tracked.	*Not Applicable*					
9.6.2.b Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented.	**Identify the sample** of recent offsite tracking logs for all media selected.	*Not Applicable*					
	For each item in the sample, **describe how** tracking details were observed to be documented.	*Not Applicable*					
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.6.3 Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals).	**Identify the responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals).	*Not Applicable. Sangoma under Doc-1 and Doc-3 has no media which contains CHD stored, nor any CHD on paper media, in its environment.*					
	For each item in the sample in 9.6.2.b, **describe how** proper management authorization was observed to be obtained whenever media is moved from a secured area (including when media is distributed to individuals).	*Not Applicable*					
9.7 Maintain strict control over the storage and accessibility of media.			☒	☐	☐	☐	☐
9.7 Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.	**Identify the documented policy for controlling storage and maintenance of all media** that was reviewed to verify that the policy defines required periodic media inventories.	*Doc-1* *Doc-3*					
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.			☒	☐	☐	☐	☐
9.7.1 Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually.	**Identify the media inventory logs** reviewed.	*Doc-14*					
	Describe how the media inventory logs verified that:						
	• Media inventory logs of all media were observed to be maintained.	*I read Doc-14 to find that server inventories are kept for all Sample Set-16 and Sample Set-18 locations. I observed that no movement of media had occurred in previous 12 months.*					
	• Media inventories are performed at least annually.	*I observed that Doc-14 was dated 19 Jan 2024, which was within the previous 12 months.*					
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.8 Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following: • Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. • Storage containers used for materials that are to be destroyed must be secured. • Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	**Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following: • Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. • Storage containers used for materials that are to be destroyed must be secured. • Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	*Doc-3*				
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.			☐	☐	☒	☐	☐
9.8.1.a Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	**Identify the responsible personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.	*Not Applicable. I learned by interview with Int-1 that Sangoma has no hard-copy CHD anywhere in its environment.*					
	Provide the name of the assessor who attests that the procedures state that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed.	*Not Applicable*					
9.8.1.b Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured.	**Describe how** the storage containers used for materials to be destroyed were verified to be secured.	*Not Applicable*					
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.8.2 Verify that cardholder data on electronic media is rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	**Describe how** cardholder data on electronic media is rendered unrecoverable, via secure wiping of media and/or physical destruction of media.	*Not Applicable. I learned by interview with Int-1 that Sangoma has no electronic or hard copy CHD anywhere in its environment.*					
	If data is rendered unrecoverable via secure deletion or a secure wipe program, **identify the industry-accepted standards** used.	*Not Applicable*					
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note:*** *These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*			☐	☐	☒	☐	☐
9.9 Examine documented policies and procedures to verify they include: • Maintaining a list of devices. • Periodically inspecting devices to look for tampering or substitution. • Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices.	**Identify the documented policies and procedures** examined to verify they include: • Maintaining a list of devices. • Periodically inspecting devices to look for tampering or substitution. • Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices.	*Not Applicable. I interviewed Int-1 and reviewed Doc-1 and determined that Sangoma has no cardholder payment flows that it manages, including payment flows with point of sale devices.*					
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device. • Location of device (for example, the address of the site or facility where the device is located). • Device serial number or other method of unique identification.			☐	☐	☒	☐	☐
9.9.1.a Examine the list of devices to verify it includes: • Make, model of device. • Location of device (for example, the address of the site or facility where the device is located). • Device serial number or other method of unique identification.	**Identify the documented up-to-date list of devices** examined to verify it includes: • Make, model of device. • Location of device (for example, the address of the site or facility where the device is located). • Device serial number or other method of unique identification.	*Not Applicable. I interviewed Int-1 and reviewed Doc-1 and determined that Sangoma has no cardholder payment flows that it manages, including payment flows with point of sale devices.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.9.1.b Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date.	**Identify the sample** of devices from the list selected for this testing procedure.	*Not Applicable*					
	For all items in the sample, **describe how** the devices and device locations were observed to verify that the list is accurate and up-to-date.	*Not Applicable*					
9.9.1.c Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc.	**Identify the responsible personnel** interviewed who confirm the list of devices is updated when devices are added, relocated, decommissioned, etc.	*Not Applicable*					
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). **Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.			☐	☐	☒	☐	☐
9.9.2.a Examine documented procedures to verify processes are defined to include the following: • Procedures for inspecting devices. • Frequency of inspections.	**Identify the documented procedures** examined to verify that processes are defined to include the following: • Procedures for inspecting devices. • Frequency of inspections.	*Not Applicable. I interviewed Int-1 and reviewed Doc-1 and determined that Sangoma has no cardholder payment flows that it manages, including payment flows with point of sale devices.*					
9.9.2.b Interview responsible personnel and observe inspection processes to verify: • Personnel are aware of procedures for inspecting devices. • All devices are periodically inspected for evidence of tampering and substitution.	**Identify** the **responsible personnel** interviewed who confirm that: • Personnel are aware of procedures for inspecting devices. • All devices are periodically inspected for evidence of tampering and substitution.	*Not Applicable*					
	Describe how inspection processes were observed to verify that:						
	• All devices are periodically inspected for evidence of tampering.	*Not Applicable*					
	• All devices are periodically inspected for evidence of substitution.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).			☐	☐	☒	☐	☐
9.9.3.a Review training materials for personnel at point-of-sale locations to verify it includes training in the following: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Not to install, replace, or return devices without verification. • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	**Identify the training materials for personnel at point-of-sale locations** that were reviewed to verify the materials include training in the following: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Not to install, replace, or return devices without verification. • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Reporting all suspicious behavior to appropriate personnel (for example, a manager or security officer). • Reporting tampering or substitution of devices.	*Not Applicable. I interviewed Int-1 and reviewed Doc-1 and determined that Sangoma has no cardholder payment flows that it manages, including payment flows with point of sale devices.*					
9.9.3.b Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to	**Identify the sample** of personnel at point-of-sale locations interviewed.	*Not Applicable*					
	For the interview, **summarize the relevant details** discussed that verify interviewees have received training and are aware of the procedures for the following:						
	• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/CCW	N/A	Not Tested	Not in Place
granting them access to modify or troubleshoot devices. • Not to install, replace, or return devices without verification. • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	• Not to install, replace, or return devices without verification.	*Not Applicable*					
	• Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).	*Not Applicable*					
	• Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	*Not Applicable*					
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
9.10 Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are: • Documented, • In use, and • Known to all affected parties.	**Identify the document reviewed to** verify that security policies and operational procedures for restricting physical access to cardholder data are documented.	*Doc-1* *Doc-7*					
	Identify the **responsible personnel interviewed** who confirm that the above documented security policies and operational procedures for restricting physical access to cardholder data are: • In use, and • Known to all affected parties.	*Int-1*					

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.1 Implement audit trails to link all access to system components to each individual user.			☒	☐	☐	☐	☐
10.1 Verify, through observation and interviewing the system administrator, that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users.	**Identify the system administrator(s)** interviewed who confirm that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users.	*Int-1* *Int-2* *Int-3*					
	Describe how audit trails were observed to verify the following:						
	• Audit trails are enabled and active for system components.	*I asked Int-1 for assistance and was shown the logging daemons on Sample Set-4 during Zoom session and found the logging daemon running (Rsyslog 8.2204.0-3.fc37) for all servers in the sample set. I asked Int-3 for review of system logging in Sample Set-6 and found log data for networking devices in Sample Set-1. Int-1 confirmed that logging is set up in Sample Set-2 to send via syslog all data to the central log platform and he also confirmed this was occurring by showing examples of it in Sample Set-6.*					
	• Access to system components is linked to individual users.	*I observed Sample Set-6 with assistance from Int-1 and Int-2. As a standard syslog platform, it is configured to show as part of its format the uid of individual users, which I observed in Sample Set-6.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2 Implement automated audit trails for all system components to reconstruct the following events:			☒	☐	☐	☐	☐

10.2 Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	**Identify the responsible personnel** interviewed who confirm the following from 10.2.1-10.2.7 are logged:
	• All individual access to cardholder data.
	• All actions taken by any individual with root or administrative privileges.
	• Access to all audit trails.
	• Invalid logical access attempts.
	• Use of and changes to identification and authentication mechanisms, including:
	  ○ All elevation of privileges.
	  ○ All changes, additions, or deletions to any account with root or administrative privileges.
	• Initialization of audit logs.
	• Stopping or pausing of audit logs.
	• Creation and deletion of system level objects.
		Int-1
		Int-2					

	Identify the sample of audit logs selected for 10.2.1-10.2.7.	*Sample Set-17*					
10.2.1 All individual user accesses to cardholder data.			☐	☐	☒	☐	☐
10.2.1 Verify all individual access to cardholder data is logged.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all individual access to cardholder data is logged.	*Not Applicable. I confirmed by interview with Int-1 that Sangoma has no cardholder data environment that it manages as part of its business model.*					
10.2.2 All actions taken by any individual with root or administrative privileges.			☒	☐	☐	☐	☐
10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all actions taken by any individual with root or administrative privileges are logged.	*I reviewed the configuration for Rsyslog 8.2204.0-3.fc37 in Sample Set-4 during live Zoom session, and found that the Rsyslog daemon was running in all serves. I looked at the logs from Sample Set-17, and found that individual actions of administrators, as well as those becoming the root account, were being logged.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2.3 Access to all audit trails.			☒	☐	☐	☐	☐
10.2.3 Verify access to all audit trails is logged.	*For all items in the sample at 10.2*, **describe how** audit logs and audit log settings verified that access to all audit trails is logged.	*I observed Sample Set-1 and Sample Set-2 during Zoom session required TACACS+ login for all access. Once access is granted, it created a logged entry via the syslog protocol on every device being accessed, as seen in Sample Set-17. I observed in Sample Set-4 that only senior engineers are allowed to log in, and each log in event which accessed audit trails is logged by Sample Set-17.*					
10.2.4 Invalid logical access attempts.			☒	☐	☐	☐	☐
10.2.4 Verify invalid logical access attempts are logged.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that invalid logical access attempts are logged.	*I observed during live Zoom session Sample Set-1 and Sample Set-2 required TACACS+ login for all access. If an invalid attempt occurs, it created a logged entry via the syslog protocol on every device being accessed, as seen in Sample Set-17. I observed in Sample Set-4 test invalid events provided by Int-1 to demonstrate that invalid events are logged by Sample Set-17.*					
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.			☒	☐	☐	☐	☐
10.2.5.a Verify use of identification and authentication mechanisms is logged.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that use of identification and authentication mechanisms is logged.	*I observed Rsyslog is running in the sample servers (Sample Set-4), and Rsyslog is configured in /etc/syslog to log all authentication attempts. I observed that the logging protocol is enabled in Sample Set-1 and Sample Set-2 and configured to log to the logging platform (Sample Set-17).*					
10.2.5.b Verify all elevation of privileges is logged.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all elevation of privileges is logged.	*I observed that Rsyslog is configured in /etc/syslog to log all elevated privilege incidents on all servers in Sample Set-4. I observed that Int-1 switched from exec mode to enable mode in demonstrations on Sample Set-1, and Sample Set-2 , and that these all logged the event to the logging platform (Sample Set-17).*					
10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that all changes, additions, or deletions to any account with root or administrative privileges are logged.	*I saw a test change to an administrative account get logged by Rsyslog, and this is standard behavior for Rsyslog configured on all servers in Sample Set-5*					
10.2.6 Initialization, stopping, or pausing of the audit logs.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.2.6 Verify the following are logged: • Initialization of audit logs. • Stopping or pausing of audit logs.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that initialization of audit logs is logged.	*Rsyslog logs a line in the log file to mark an initialization event in all cases of initialization. This was seen in a sample of initialization events in Sample Set-17.*					
	For all items in the sample at 10.2, **describe how** audit logs and audit log settings verified that stopping and pausing of audit logs is logged.	*Logwatch is used to alert to changes to Rsyslog. In Sample Set-17, I observed Logwatch report on stopping/pausing Rsyslog.*					
10.2.7 Creation and deletion of system-level objects.			☒	☐	☐	☐	☐
10.2.7 Verify creation and deletion of system level objects are logged.	*For all items in the sample at 10.2,* **describe how** audit logs and audit log settings verified that creation and deletion of system level objects are logged.	*OSSEC is configured to watch directories like /etc and /usr/bin where system configuration files and system objects are located. A test incident was logged and seen in Sample Set-17.*					
10.3 Record at least the following audit trail entries for all system components for each event:			☒	☐	☐	☐	☐
10.3 Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	**Identify the responsible personnel** interviewed who confirm that for each auditable event from 10.2.1-10.2.7, the following are included in log entries: • User identification • Type of event • Date and time • Success or failure indication • Origination of event	*Int-1* *Int-2*					
	Identify the sample of audit logs from 10.2.1-10.2.7 observed to verify the following are included in log entries: • User identification • Type of event • Date and time • Success or failure indication • Origination of event	*Sample Set-17*					
10.3.1 User identification			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.3.1 Verify user identification is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that user identification is included in log entries.	*I read samples in Sample Set-17 to see users who log into servers get logged into the log files created with Rsyslog. Logwatch and OSSEC also logged UID when they created a log incident sent to Rsyslog.*					
10.3.2 Type of event			☒	☐	☐	☐	☐
10.3.2 Verify type of event is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that type of event is included in log entries.	*I read logs in the sample, and observed login, logout, IP connections, email sent, and date and time changes were logged using Rsyslog "info" level. All incidents were sent immediately to the syslog file generated by the Rsyslog daemon and sent to Sample Set-17 using the syslog protocol.*					
10.3.3 Date and time			☒	☐	☐	☐	☐
10.3.3 Verify date-and-time stamp is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that date and time stamp is included in log entries.	*I observed in Sample Set-17 that date and time stamp were included in every logged entry created by Rsyslog by Logwatch, and by OSSEC.*					
10.3.4 Success or failure indication			☒	☐	☐	☐	☐
10.3.4 Verify success or failure indication is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that success or failure indication is included in log entries.	*I observed in Sample Set-17 that success and failure of incidents such as logins and connection attempts to running processes were logged by Rsyslog. OSSEC attempts to write to watched directories was logged. Creation or removal of log files was alarmed by Logwatch.*					
10.3.5 Origination of event			☒	☐	☐	☐	☐
10.3.5 Verify origination of event is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that origination of event is included in log entries.	*I observed in Sample Set-17 that the origination of event by IP address is a built-in fact of all Rsyslog entries, including the ones in Sample Set-17.*					
10.3.6 Identity or name of affected data, system component, or resource			☒	☐	☐	☐	☐
10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	*For all logs in the sample at 10.3,* **describe how** the audit logs verified that the identity or name of affected data, system component, or resource is included in log entries.	*I observed in Sample Set-17 that the syslog format in use by Rsyslog includes a detail of what daemon, service, process is creating the incident is captured in all logged events, including the logged events in Sample Set-17.*					
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.4 Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	**Identify** the time-synchronization technologies in use. (If NTP, include version)	*NTP v4.2*					
	Identify the documented time-synchronization configuration standards examined to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	*Doc-6* *Doc-19* *Doc-21*					
	Describe how processes were examined to verify that time synchronization technologies are:						
	• Implemented.	*I observed with assistance from Int-1 during live Zoom session that all devices at Sangoma are using ntp.conf files that contain time-a and time-b (NIST) and US Navy tic/toc backup. I observed this in their NTP daemon configuration files, as part of observation in Sample Set-1, Sample Set-2 and Sample Set-4, with Int-1's assistance, to pull time from these industry-recognized sources., as documented in Doc-6 and Doc-21.*					
	• Kept current, per the documented process.	*I observed with Int-1 assistance during live Zoom session to show the NTP configuration files in the devices in Sample Set-1, Sample Set-2 and Sample Set-4. All devices are built to use these round-robin time sources provided by NIST and US Navy, and they are kept current by standard patching practice (Doc-19) at Sangoma.*					
10.4.1 Critical systems have the correct and consistent time.			☒	☐	☐	☐	☐
10.4.1.a Examine the process for acquiring, distributing and storing the correct time within the organization to verify that: • Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the time servers	**Describe how** the process for acquiring, distributing, and storing the correct time within the organization was examined to verify the following:						
	▪ Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	*I observed that all devices in Sample Set-1, Sample Set-2, Sample Set-4 and Sample Set-6 are configured to receive time from the NIST and US Navy time servers.*					
	▪ Where there is more than one designated time server, the time servers peer with one another to keep accurate time.	*Not Applicable. Sangoma does not rely on multiple servers within its network, but rather configures to pull NTP from the NIST and US Navy time server platforms.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
peer with one another to keep accurate time. • Systems receive time information only from designated central time server(s).	▪ Systems receive time information only from designated central time server(s).	*I observed with assistance from Int-1 that Sangoma servers receive time from the designated NIST or US Navy time server platforms only by default configuration which is not changed.*					
10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify: • Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. • Systems receive time only from designated central time server(s).	**Identify the sample** of system components selected for 10.4.1.b-10.4.2.b	*Sample Set-1* *Sample Set-2* *Sample Set-4* *Sample Set-6*					
	For all items in the sample, **describe how** the time-related system-parameter settings verified:						
	▪ Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.	*I observed that Sample Set-2, which are the central time routers designated, are configured to receive time from UTC.*					
	▪ Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.	*Not Applicable. Sangoma does not rely on multiple servers within its network, but rather configures to pull NTP from the NIST and US Navy time server platforms.*					
	▪ Systems receive time only from designated central time server(s).	*I observed with assistance from Int-1 that all Sangoma servers receive time from the designated NIST or US Navy time server platforms only by default configuration which is not changed.*					
10.4.2 Time data is protected.			☒	☐	☐	☐	☐
10.4.2.a Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.	*For all items in the sample from 10.4.1,* **describe how** configuration settings verified that access to time data is restricted to only personnel with a business need to access time data.	*I read Doc-2 to learn that locked file permissions were documented for server operating system data including time data. I read Doc-13 to observe that 'hardening' or locking file permissions is required by Sangoma. I observed with assistance from Int-1 that the ntp.conf configuration is locked to permissions, which matched the documented example in Doc-2 There are no business needs defined to edit the ntp.conf file on Sample Set-4 Sangoma servers. On network devices in Sample Set-1 and Sample Set-2, only senior engineering employees (Int-1, Int-2) are allowed access to the devices at all, as they have a documented need to be able to log in.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.4.2.b Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	*For all items in the sample from 10.4.1,* **describe how** configuration settings and time synchronization settings verified that any changes to time settings on critical systems are logged.	*I observed ntp.conf as part of Sample Set-4 and observed that OSSEC is configured to monitor any changes to time settings. Alarms will be received into the Rsyslog 8.2204.0-3.fc37 system, and also alerted upon to Security staff.*					
	For all items in the sample from 10.4.1, **describe how** the examined logs verified that any changes to time settings on critical systems are logged.	*I observed with assistance from Int-1 during live Zoom session that a test time-change was performed on a server in Sample Set-4 and a firewall in Sample Set-1 and results noted.*					
	Describe how time synchronization processes were examined to verify changes to time settings on critical systems are:						
	• Logged	*I observed with assistance from Int-1 that OSSEC during Zoom session is configured to record a time change incident. Rsyslog captures the log file. I observed Sample Set-6 Logwatch with assistance from Int-1 and found that time entries were being received from Sample Set-1, Sample Set-2, and Sample Set-4.*					
	• Monitored	*I observed with assistance from Int-1 that OSSEC is configured to alert to the Security alias email if a time change occurs. Logwatch alerted in a sample time change in Sample Set-1 provided by Int-1.*					
	• Reviewed	*I observed with assistance from Int-1 that email to Security group is reviewed by on-call security team member.*					
10.4.3 Time settings are received from industry-accepted time sources.			☒	☐	☐	☐	☐
10.4.3 Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	**Identify the sample** of time servers selected for this testing procedure.	*Sample Set-2*					
	For all items in the sample, **describe how** configuration settings verified either of the following:						
	• That the time servers receive time updates from specific, industry-accepted external sources. OR	*I observed with assistance from Int-1 that time-a, time-b (NIST) and "tic / toc" (US Navy) are time platform provided by industry-standard servers.*					
	• That time updates are encrypted with a symmetric key, and access control lists specify the IP addresses of client machines.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.5 Secure audit trails so they cannot be altered.			☒	☐	☐	☐	☐
10.5 Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:	**Identify the system administrators** interviewed who confirm that audit trails are secured so that they cannot be altered as follows (from 10.5.1-10.5.5): • Only individuals who have a job-related need can view audit trail files. • Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. • Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, including: – That current audit trail files are promptly backed up to the centralized log server or media – The frequency that audit trail files are backed up – That the centralized log server or media is difficult to alter • Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. • Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.	*Int-1* *Int-2*				
	Identify the sample of system components selected for 10.5.1-10.5.5.	*Sample Set-4*					
10.5.1 Limit viewing of audit trails to those with a job-related need.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.5.1 Only individuals who have a job-related need can view audit trail files.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that only individuals who have a job-related need can view audit trail files.	*I observed with assistance from Int-1 using live Zoom session that Administrators in the privileged (wheel) group in Sample Set-4 only are allowed access to audit trails on Sangoma servers. I observed the wheel group[membership for privileged users, and the permissions on the server /var/log/secure directory to confirm these details.*					
10.5.2 Protect audit trail files from unauthorized modifications.			☒	☐	☐	☐	☐
10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	*I observed during live Zoom session that on all servers in Sample Set-4 /var/log/secure is set to not allow user read-write access. This is standard build configuration for all Sangoma servers observed.*					
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.			☒	☐	☐	☐	☐
10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	*I observed during live Zoom session that logs are sent to a logging server platform in Sangoma VLAN immediately using the syslog protocol on port 514. These directories are kept for at least one year. Backups are made by copying these directory files to a second server repository located in Sangoma administrative VLAN. IP address limits on access to the server platform, and 'wheel' membership to only privileged users, results in a server platform that is not alterable by any but authorized administrators. The syslog directory itself is writable only by the syslog daemon. No administrators may easily write to the backup directories.*					
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.			☐	☐	☒	☐	☐
10.5.4 Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media.	*For each item in the sample at 10.5,* **describe how** system configurations and permissions verified that logs for external-facing technologies are written onto a secure, centralized, internal log server or media.	*Not Applicable. I learned by interview with Int-1 and Int-2 and observing logs in Sample Set-4 that Sangoma has no external-facing technologies in use in the in-scope environment.*					
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.5.5 Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.	*For each item in the sample at 10.5,* **describe how** the following verified the use of file-integrity monitoring or change-detection software on logs:						
	• System settings	*I reviewed OSSEC configuration with assistance from Int-1 and observed it is configured to include system configuration directory.*					
	• Monitored files	*I reviewed the sample set and observed that Logwatch is configured to monitor any changes to log files, and to alert the Security group in this event.*					
	• Results from monitoring activities	*I observed that Logwatch alerts on any changes to the syslog monitoring on the platform.*					
	Identify the file-integrity monitoring (FIM) or change-detection software verified to be in use.	*Logwatch*					
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*							
10.6 Perform the following:							
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).			☒	☐	☐	☐	☐
10.6.1.a Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components	**Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions.	*Doc-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**Describe** the manual or log tools used for daily review of logs.	*I observed during live Zoom session that Logwatch was in use by Sangoma administrators to receive automated log reporting by email.*					
10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	**Identify the responsible personnel** interviewed who confirm that the following are reviewed at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions.	*Int-2* *Int-3* *Int-4*					
	Describe how processes were observed to verify that the following are reviewed at least daily:						
	• All security events.	*I observed during live Zoom review with Int-1 and Int-2 that Logwatch alerting in the form of alert emails is in place on servers in Sample Set-4. Test alerts were performed by creating a test login event as I observed the administrative alert email get sent to those in the Operations group.*					
	• Logs of all system components that store, process, or transmit CHD and/or SAD.	*Not Applicable. Sangoma has no environment that it maintains which stores, processes, or transmits CHD.*					
	• Logs of all critical system components.	*I observed in Sample Set-4 during live Zoom session with Int-1 and Int-2 that Logwatch and OSSEC alert emails on incidents in syslog which affect system binaries and system configuration files were sent to Operations mail.*					
	• Logs of all servers and system components that perform security functions.	*I observed during live Zoom session demonstration with Int-1 and Int-2 and by being shown configuration file OSSEC configuration and by observing Logwatch logging to confirm that Logwatch and OSSEC alert on servers existed on every server in Sample Set-4.*					
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.6.2.a Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy.	**Identify the documented security policies and procedures** examined to verify that procedures define reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy.	*Doc-1*					
	Describe the manual or log tools defined for periodic review of logs of all other system components.	*I observed with assistance from Int-1 and Int-2 by live Zoom login session shown to me that OSSEC was running on servers, and that Int-1 and Int-2 said that it was used for alerts. I observe that it was running by having Int-1 perform a ps -ef on servers in Sample Set-4 to display running processes, and Int-2 displayed a daily log summary report email which was produced by Rsyslog and Logwatch.*					
10.6.2.b Examine the organization's risk assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.	**Identify the organization's risk assessment documentation** examined to verify that reviews are performed in accordance with the organization's policies and risk management strategy.	*Doc-19*					
	Identify the responsible personnel interviewed who confirm that reviews are performed in accordance with organization's policies and risk management strategy.	*Int-1* *Int-2*					
10.6.3 Follow up exceptions and anomalies identified during the review process.			☒	☐	☐	☐	☐
10.6.3.a Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.	**Identify the documented security policies and procedures** examined to verify that procedures define following up on exceptions and anomalies identified during the review process.	*Doc-1*					
10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.	**Describe how** processes were observed to verify that follow-up to exceptions and anomalies is performed.	*I observed Security email follow-up folder shown by Int-1 as part of daily log review process and confirmed that follow-up is performed by Security group or by a designate of that group.*					
	Identify the responsible personnel interviewed who confirm that follow-up to exceptions and anomalies is performed.	*Int-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).			☒	☐	☐	☐	☐
10.7.a Examine security policies and procedures to verify that they define the following: • Audit log retention policies. • Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.	**Identify the documented security policies and procedures** examined to verify that procedures define the following: • Audit log retention policies. • Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.	*Doc-1*					
10.7.b Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.	**Identify the responsible personnel** interviewed who confirm that audit logs are retained for at least one year.	*Int-1* *Int-2*					
	Describe how the audit logs verified that audit logs are retained for at least one year.	*The central log repository directory in Sample Set-6 was observed to contain log files older than one year old.*					
10.7.c Interview personnel and observe processes to verify that at least the last three months' logs are immediately available for analysis.	**Identify the responsible personnel** interviewed who confirm that at least the last three months' logs are immediately available for analysis.	*Int-1* *Int-2*					
	Describe how processes were observed to verify that at least the last three months' logs are immediately available for analysis.	*I observed that Rsyslog on all servers is configured to use the syslog protocol using the Rsyslog daemon to send immediate logging to the log platform at Sangoma.*					
10.8 ***Additional requirement for service providers only*:** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.8.a Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	**Identify the documented policies and procedures** examined to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	*Doc-1*					
10.8.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	**Identify the responsible personnel** interviewed who confirm that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	*Int-1*					
	Describe how examination of the detection and alerting processes verified that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	*I observed by example provided from Int-1 setting off a test alarm that email is sent to the security group. This was demonstrated for each of the classes of devices or incidents required.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.8.1 ***Additional requirement for service providers only*:** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls			☒	☐	☐	☐	☐
10.8.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are	**Identify the documented policies and procedures** examined to verify that processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	*Doc-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	**Identify the responsible personnel** interviewed who confirm that processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	*Int-1*					
10.8.1.b Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	**Identify the sample of records** examined to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	*Sample Set-12*					
	For each sampled record, **describe how** the documented security control failures include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	*I observed that the root cause of the alert is listed in the email sent to the Engineering group. The incident start and end times are also in the alert. In the subsequent email, members of the engineering group are expected to discuss and identify the remediation, which I observed had occurred in Sample Set-12 alerting examples.*					
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
10.9 Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented.	*Doc-1*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for monitoring all access to network resources and cardholder data are: • In use • Known to all affected parties	*Int-1* *Int-2*					

Requirement 11: Regularly test security systems and processes

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*			☒	☐	☐	☐	☐
11.1.a Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis.	**Identify the documented policies and procedures** examined to verify processes are defined for detection and identification of authorized and unauthorized wireless access points on a quarterly basis.	*Doc-1* *Doc-14* *Doc-20*					
11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: • WLAN cards inserted into system components. • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). • Wireless devices attached to a network port or network device.	**Provide the name of the assessor** who attests that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: • WLAN cards inserted into system components. • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). • Wireless devices attached to a network port or network device.	*David M Dennis*					
11.1.c If wireless scanning is utilized, examine output from recent wireless scans to verify that:	**Indicate whether** wireless scanning is utilized. **(yes/no)** *If 'no,' mark the remainder of 11.1.c as 'not applicable.'*	*yes*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
• Authorized and unauthorized wireless access points are identified, and • The scan is performed at least quarterly for all system components and facilities.	*If 'yes,'* **Identify/describe** the output from recent wireless scans examined to verify that: • Authorized wireless access points are identified. • Unauthorized wireless access points are identified. • The scan is performed at least quarterly. • The scan covers all system components. • The scan covers all facilities.	*I read Doc-1 and Doc-14 and found that no Wi-Fi responsibility exists for the data center for Sangoma; this is the responsibility of the Sample Set-16 data center providers. I read Doc-14 tracking and found that these data centers had been assessed and passed this requirement.* *I observed in Sample Set-18 with assistance from Int-10 that checking for unauthorized wi-fi in these facilities is performed on a site-wide alarm basis using quarterly inspection.*					
11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel.	**Indicate whether** automated monitoring is utilized. **(yes/no)**	*yes*					
	If "no," mark the remainder of 11.1.d as "Not Applicable." *If "yes," complete the following:*						
	Identify and describe any automated monitoring technologies in use.	*I read Doc-1 and Doc-14 and found that no Wi-Fi responsibility exists for the data center for Sangoma; this is the responsibility of the Sample Set-16 data center providers. I read Doc-14 tracking and found that these data centers had been assessed by on-site and passed this requirement.* *I observed in Sample Set-18 with assistance from Int-10 that automated unauthorized wi-fi checks were not automatically performed at these sites.*					
	For each monitoring technology in use, **describe how** the technology generates alerts to personnel.	*I read Doc-1 and Doc-14 and found that no Wi-Fi responsibility exists for the data center for Sangoma; this is the responsibility of the Sample Set-16 data center providers. I read Doc-14 tracking and found that these data centers had been assessed by on-site and passed this requirement.* *I observed that Sample Set-18 did not perform this automatic monitoring by interview with Int-10.*					
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.			☒	☐	☐	☐	☐
11.1.1 Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.	**Identify the documented inventory records** of authorized wireless access points examined to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.	*Doc-14*					
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.1.2.a Examine the organization's incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected.	**Identify the Incident Response Plan document** examined that defines and requires response in the event that an unauthorized wireless access point is detected.	*Doc-1*					
11.1.2.b Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found.	**Identify the responsible personnel** interviewed for this testing procedure.	*Int-1*					
	For the interview, **summarize the relevant details** discussed that verify that action is taken when unauthorized wireless access points are found.	*I interviewed Int-1 who described that an unauthorized Wi-Fi access point found in Sample Set-16's facilities would be reported to Sangoma if it impacted Sangoma' network. This is following Sangoma incident response plan where any incident found at the co-located data centers is reported to Sangoma.* *I interviewed Int-1 and Int-10 who confirmed that in Sample Set-18, notification appropriate to any incident would be reported to Sangoma.*					
	And/or:						
	Identify the recent wireless scans inspected for this testing procedure.	*I read Doc-1 and found this responsibility to be performed by the co-located data centers in Sample Set-16. According to Doc-14, Sample Set-16 are compliant service providers that perform this role.* *I interviewed Int-1 and Int-10 to learn that Sample Set-18 was not using automated scans for unauthorized wi-fi.*					
	Describe how the recent wireless scans and related responses verified that action is taken when unauthorized wireless access points are found.	*I read Doc-1 and found this responsibility to be performed by the co-located data centers in Sample Set-16. According to Doc-14, Sample Set-16 are compliant service providers that perform this role.* *I interviewed Int-1 and Int-10 to learn that Sample Set-18 was not using automated scans for unauthorized wi-fi.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*			☒	☐	☐	☐	☐
11.2 Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as follows:							
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high-risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.			☒	☐	☐	☐	☐
11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.	**Identify the internal vulnerability scan reports and supporting documentation** reviewed.	*Doc-16* *Doc-37* *Doc-38* *Doc-39* *Doc-40* *Doc-49* *Doc-50* *Doc-51* *Doc-52*					
	Provide the name of the assessor who attests that four quarterly internal scans were verified to have occurred in the most recent 12-month period.	*David M Dennis*					
11.2.1.b Review the scan reports and verify that all "high-risk" vulnerabilities are addressed and the scan process includes rescans to verify that the "high-	**Identify the documented process for quarterly internal scanning** to verify the process defines performing rescans as part of the quarterly internal scan process.	*Doc-16*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	*For each of the four internal quarterly scans indicated at 11.2.1.a*, **indicate whether** a rescan was required. **(yes/no)**	*no*					
	If "yes," **describe how** rescans were verified to be performed until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	*Not Applicable*					
11.2.1.c Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Identify the responsible personnel** interviewed for this testing procedure.	*Int-1*					
	Indicate whether a qualified internal resource performs the scan. **(yes/no)** *If "no," mark the remainder of 11.2.1.c as "Not Applicable."* *If "yes," complete the following:*	*yes*					
	For the interview, **summarize the relevant details** discussed that verify:						
	▪ The scan was performed by a qualified internal resource	*I interviewed Int-1 and queried his credentials. I found that Int-1 had deep knowledge of the Nessus tool and had contributed to its mailing list. These led to a determination of compliance.*					
	▪ Organizational independence of the tester exists.	*I reviewed Doc-1 and interviewed Int-1 and was told that Int-1 has the authority within Sangoma to require that any security issue be addressed and is independent of the business owners of the network, who must sign off on the findings when scanned.*					
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note*:** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.2.2.a Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period.	**Identify the external network vulnerability scan reports and supporting documentation** reviewed.	*Doc-16* *Doc-31* *Doc-32* *Doc-33* *Doc-34* *Doc-57*					
	Provide the name of the assessor who attests that four quarterly external vulnerability scans were verified to have occurred in the most recent 12-month period.	*David M Dennis*					
11.2.2.b Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures).	**Provide the name of the assessor** who attests that the results of each quarterly scan were reviewed and verified that the ASV Program Guide requirements for a passing scan have been met.	*David M Dennis*					
	For each of the four external quarterly scans indicated at 11.2.2.a, **indicate whether** a rescan was necessary. **(yes/no)**	*Doc-31 22 May 2023 No* *Doc-32 22 Aug 2023 Yes* *Doc-33 14 Nov 2023 No* *Doc-34 11 Jan 2024 Yes* *Doc-57 21 Mar 2024 No*					
	If "yes," **describe how** the results of the rescan verified that the ASV Program Guide requirements for a passing scan have been met.	*I observed scan failure was due to remediation issue, which was met by following scan to confirm once properly ASV remediated by scanning ASV provider. In all cases there were no outstanding high or critical issues in the reports.*					
11.2.2.c Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	**Provide the name of the assessor** who attests that the external scan reports were reviewed and verified to have been completed by a PCI SSC-Approved Scanning Vendor (ASV).	*David M Dennis*					
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.2.3.a Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned.	**Identify the change control documentation and scan reports** reviewed for this testing procedure.	*Not Applicable. I learned from Int-1 as well as Doc-19 and Sample Set-10 and Sample Set-11 review that no significant change occurred in previous 12 months.*					
	Describe how the change control documentation and scan reports verified that all system components subject to significant change were scanned after the change.	*Not Applicable*					
11.2.3.b Review scan reports and verify that the scan process includes rescans until: • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. • For internal scans, all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.	For all scans reviewed in 11.2.3.a, **indicate whether** a rescan was required. **(yes/no)**	*no*					
	If "yes" – for external scans, **describe how** rescans were performed until no vulnerabilities with a CVSS score greater than 4.0 exist.	*Not Applicable*					
	If "yes" – for internal scans, **describe how** rescans were performed until either passing results were obtained or all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 were resolved.	*Not Applicable*					
11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Indicate whether** an **i**nternal resource performed the scans. **(yes/no)** *If "no," mark the remainder of 11.2.3.c as "Not Applicable."* *If "yes," complete the following:*	*no*					
	Describe how the personnel who perform the scans demonstrated they are qualified to perform the scans.	*Not Applicable*					
	Describe how organizational independence of the tester was observed to exist.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.3 Implement a methodology for penetration testing that includes at least the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). • Includes coverage for the entire CDE perimeter and critical systems. • Includes testing from both inside and outside of the network. • Includes testing to validate any segmentation and scope reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. • Specifies retention of penetration testing results and remediation activities results.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.3 Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented and includes at least the following: • Is based on industry-accepted penetration testing approaches. • Includes coverage for the entire CDE perimeter and critical systems. • Includes testing from both inside and outside the network. • Includes testing to validate any segmentation and scope reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. • Specifies retention of penetration testing results and remediation activities results.	**Identify the documented penetration-testing methodology** examined to verify a methodology is implemented that includes at least the following: • Based on industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Retention of penetration testing results and remediation activities results.	*Doc-1* *Doc-35* *Doc-36*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed who confirm the penetration–testing methodology implemented includes at least the following: • Based on industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Retention of penetration testing results and remediation activities results.	*Int-1*					
11.3.1 Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).			☒	☐	☐	☐	☐
11.3.1.a Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: • Per the defined methodology • At least annually • After any significant changes to the environment	**Identify the documented external penetration test results** reviewed to verify that external penetration testing is performed: • Per the defined methodology • At least annually	*Doc-35*					
	Describe how the scope of work verified that external penetration testing is performed: • Per the defined methodology • At least annually	*I reviewed Doc-35 and compared it to Doc-1 to confirm the methodology was followed and interviewed Int-2 who confirmed that the scope of work is followed and that they conducted testing on a semi-yearly basis. I observed in Doc-35 that semi-yearly was the requirement specified for Sangoma.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify whether any significant external infrastructure or application upgrade or modification occurred during the past 12 months.	*Significant external changes did not occur in the previous 12 months, according to Int-1.*					
	Identify the documented penetration test results reviewed to verify that external penetration tests are performed after significant external infrastructure or application upgrade.	*Not Applicable. I interviewed Int-1 and reviewed Sample Set-1, Sample Set-2, and Sample Set-4 to determine that significant changes to the externally facing environment did not occur in the previous year.*					
11.3.1.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Indicate whether** an **i**nternal resource performed the test. **(yes/no)** *If "no," mark the remainder of 11.3.1.b as "Not Applicable."* *If "yes," complete the following:*	*no*					
	Describe how the personnel who perform the penetration tests demonstrated they are qualified to perform the tests.	*Not Applicable*					
	Describe how organizational independence of the tester was observed to exist.	*Not Applicable*					
11.3.2 Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).			☒	☐	☐	☐	☐
11.3.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows: • Per the defined methodology • At least annually • After any significant changes to the environment	**Identify the documented internal penetration test results** reviewed to verify that internal penetration testing is performed: • Per the defined methodology • At least annually	*Doc-29* *Doc-36*					
	Describe how the scope of work verified that internal penetration testing is performed: • Per the defined methodology • At least annually	*I read Doc-1 and found that it penetration testing was required at least annually, and to follow the defined methodology, which included attempts to gain unauthorized access, extract sensitive data, and run remote commands. I read Doc-29 and Doc-36 and observed that these steps were performed in both tests. These topics were covered by the report and reported to have been unsuccessful.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Indicate whether any significant internal infrastructure or application upgrade or modification occurred during the past 12 months. **(yes/no)**	*no*					
	Identify the documented internal penetration test results reviewed to verify that internal penetration tests are performed after significant internal infrastructure or application upgrade.	*Doc-29* *Doc-36*					
11.3.2.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Indicate whether** an **i**nternal resource performed the test. **(yes/no)** *If "no," mark the remainder of 11.3.2.b as "Not Applicable."* *If "yes," complete the following:*	*no*					
	Describe how the personnel who perform the penetration tests demonstrated they are qualified to perform the tests	*Not Applicable*					
	Describe how organizational independence of the tester was observed to exist.	*Not Applicable*					
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.			☒	☐	☐	☐	☐
11.3.3 Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	**Identify the documented penetration testing results** examined to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	*Doc-29* *Doc-35* *Doc-36*					
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.			☐	☐	☐	☐	☐
11.3.4.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all	**Indicate whether** segmentation is used to isolate the CDE from other networks. **(yes/no)** *If "no," mark the remainder of 11.3.4.a, 11.3.4.b and 11.3.4.c as "Not Applicable."*	*yes*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	*If "yes,"* **identify the defined penetration-testing methodology** examined to verify procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	*I read Doc-29 and Doc-36 and found that it made use of testing for "arp cache poisoning" exposure, as well as tested for VLAN boundaries.*					
	Describe how the segmentation controls verified that segmentation methods:						
	▪ Are operational and effective.	*I observed during live Zoom session that Sample Set-1 ACL and VLAN definitions and found that Doc-29 and Doc-36 attempted to cross these boundaries by a method called ARP (Address Resolution Protocol) cache poisoning or putting bad values into the network origin of IP addresses and seeing if it could traverse VLAN or ACL boundaries. The failure of this method indicated that segmentation methods were operational and effective.*					
	▪ Isolate all out-of-scope systems from systems in the CDE.	*I observed that the Doc-29 and Doc-36 test considered all systems in Sample Set-4 to be in scope and tested based on this assumption. The failure to compromise any system indicated that the in-scope network could not be compromised.*					
11.3.4.b Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**Identify the documented results from the most recent penetration test** examined to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	*Doc-35* *Doc-36*					
11.3.4.c Verify that the test was performed by a qualified internal resource or qualified external third party,	**Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests.	*I interviewed Int-1 who confirmed that VikingCloud was used for penetration testing. I read Doc-35 and Doc-36 and confirmed this. VikingCloud is an industry-accepted source of these services.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Describe how** organizational independence of the tester was observed to exist.	*I interviewed Int-1 who described that the penetration tester has a scope of work that is independent of any organizational interest within Sangoma.*					
11.3.4.1 ***Additional requirement for service providers only*****:** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.			☒	☐	☐	☐	☐
11.3.4.1.a Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**Identify the documented results from the most recent penetration test** examined to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	*Doc-35* *Doc-36*					
11.3.4.1.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**Describe how** the personnel who perform the penetration tests demonstrated they are qualified to perform the tests.	*I read the scope of work and testing methodologies in Doc-35 and Doc-36, and they were provided by VikingCloud. VikingCloud is an industry-accepted source that is known to be qualified to perform penetration testing.*					
	Describe how organizational independence of the tester was observed to exist.	*I observed that the testing company was not employees of Sangoma and were producing report results outside of input from Sangoma employees or executives.*					
11.4 Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.4.a Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: • At the perimeter of the cardholder data environment. • At critical points in the cardholder data environment.	**Identify the network diagrams** examined to verify that techniques are in place to monitor all traffic: • At the perimeter of the cardholder data environment. • At critical points in the cardholder data environment.	*Doc-42* *Doc-43* *Doc-44*					
	Describe how system configurations verified that techniques are in place to monitor all traffic:						
	• At the perimeter of the cardholder data environment.	*I observed during live Zoom review the VLAN and ACL definitions in Sample Set-1 and Sample Set-2 were defined to separate the customer edge from the administrative network.*					
	• At critical points in the cardholder data environment.	*Not Applicable. Sangoma has an administrative network, but no cardholder data is present.*					
11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	**Describe how** system configurations for intrusion-detection and/or intrusion-prevention techniques verified that they are configured to alert personnel of suspected compromises.	*I observed that OSSEC was installed and running on all servers in Sample Set-4. I observed that OSSEC sent its logs to Logwatch, which in turn alerted members of the Security / wheel group of any incident.*					
	Identify the responsible personnel interviewed who confirm that the generated alerts are received as intended.	*Int-1* *Int-2*					
11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	**Identify the vendor document(s)** examined to verify defined vendor instructions for intrusion-detection and/or intrusion-prevention techniques.	*https://www.ossec.net/docs/docs/manual/index.html*					
	Describe how IDS/IPS configurations and vendor documentation verified that intrusion-detection, and/or intrusion-prevention techniques are:						
	• Configured per vendor instructions to ensure optimal protection.	*I observed in Sample Set-4 that the OSSEC agents were installed on all servers and configured to monitor all directories containing sensitive system files, configuration files or binaries.*					
	• Maintained per vendor instructions to ensure optimal protection.	*I observed in Sample Set-4 that the OSSEC agents were maintained with appropriate permissions on all servers, and configured to monitor directories containing sensitive system files, configuration files or binaries.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• Updated per vendor instructions to ensure optimal protection.	*I observed that OSSEC installed in Sample Set-4 was configured to automatically install new rules when updates were installed in ossec.conf.*					
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or* service provider*).*			☒	☐	☐	☐	☐
11.5.a Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. *Examples of files that should be monitored:* • *System executables* • *Application executables* • *Configuration and parameter files* • *Centrally stored, historical or archived, log and audit files* • *Additional critical files determined by entity (i.e., through risk assessment or other means)*	**Describe** the change-detection mechanism deployed.	*I asked Int-1 as part of the live sessions to review running processes on sampled servers in Sample Set-4 and found in each cast that in each case in Sample Set-4, OSSEC change detection software is installed on all linux servers in the environment.*					
	Identify the results from monitored files reviewed to verify the use of a change-detection mechanism.	*I asked Int-1 as part of the live sessions to review running processes on sampled servers in Sample Set-4 and found in each cast that in each case in Sample Set-6, OSSEC logs results to syslog using the Rsyslog daemon.*					
	Describe how the following verified the use of a change-detection mechanism:						
	• System settings	*I read the OSSEC.conf configuration shown to me by Int-1 during live Zoom session and found it was set up the same on all servers in the sample set, to monitor /bin, /usr/bin, and the /opt directories.*					
	• Monitored files	*I read the OSSEC.conf configuration shown to me by Int-1 during live Zoom session and found it was set up the same on all servers in the sample set, to monitor /etc configuration directory.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
11.5.b Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly.	**Describe how** system settings verified that the change-detection mechanism is configured to:						
	• Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files.	*I observed during live Zoom review of a test incident staged on a server to create an unauthorized software incident test, which emailed results to the Security group.*					
	• Perform critical file comparisons at least weekly.	*OSSEC is configured to check directories weekly per Int-1 and per review of OSSEC.conf on the Sample Set-4 servers.*					
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.			☒	☐	☐	☐	☐
11.5.1 Interview personnel to verify that all alerts are investigated and resolved.	**Identify the responsible personnel** interviewed who confirm that all alerts are investigated and resolved	*Int-1*					
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.			☒	☐	☐	☐	☐
11.6 Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are: • Documented, • In use, and • Known to all affected parties.	**Identify the document** reviewed to verify that security policies and operational procedures for security monitoring and testing are documented.	*Doc-1*					
	Identify the responsible personnel interviewed who confirm that the above documented security policies and operational procedures for security monitoring and testing are: • In use • Known to all affected parties	*Int-1* *Int-2*					

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.1 Establish, publish, maintain, and disseminate a security policy.			☒	☐	☐	☐	☐
12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	**Identify the documented information security policy** examined.	*Doc-1*					
	Describe how the information security policy was verified to be published and disseminated to:						
	• All relevant personnel.	*Int-1 has responsibility to ensure all employees of Sangoma are familiar with the security policies. They perform this by providing the policy on the internal Wiki (CRM) site with many sub-policies being made available and regularly updated.*					
	• All relevant vendors and business partners.	*Business partners and vendors are required to comply with relevant Sangoma policies, according to Int-1, and business partners receive a written notice of this as part of their signed contract with Sangoma onboarding.*					
12.1.1 Review the security policy at least annually and update the policy when business objectives or the risk environment change.			☒	☐	☐	☐	☐
12.1.1 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.	**Describe how** the information security policy was verified to be:						
	• Reviewed at least annually.	*I read Doc-1 and found that it was reviewed last date is 8 Nov 2023, within a year. This is under policy to review annually.*					
	• Updated as needed to reflect changes to business objectives or the risk environment.	*I interviewed Int-1 who confirmed that the review of all policies covered by this Doc-1 policy reflects evolving objectives.*					
12.2 Implement a risk assessment process, that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.2.a Verify that an annual risk-assessment process is documented that: • Identifies critical assets, threats, and vulnerabilities • Results in a formal, documented analysis of risk.	**Provide the name of the assessor** who attests that the documented annual risk-assessment process: • Identifies critical assets, threats, and vulnerabilities • Results in a formal, documented analysis of risk.	*David M Dennis*					
12.2.b Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	**Identify the risk assessment result documentation** reviewed to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	*Doc-18* *Doc-19*					
12.3 Develop usage policies for critical technologies and define proper use of these technologies. ***Note:*** *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following:			☒	☐	☐	☐	☐
12.3 Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed:	**Identify** critical technologies in use.	*Internet usage* *E-mail usage* *Laptop computers* *VPN usage*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the usage policies for all identified critical technologies reviewed to verify the following policies (12.3.1-12.3.10) are defined: • Explicit approval from authorized parties to use the technologies. • All technology use to be authenticated with user ID and password or other authentication item. • A list of all devices and personnel authorized to use the devices. • A method to accurately and readily determine owner, contact information, and purpose. • Acceptable uses for the technology. • Acceptable network locations for the technology. • A list of company-approved products. • Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. • Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. • Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	*Doc-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the responsible personnel interviewed who confirm usage policies for all identified critical technologies are implemented and followed (for 12.3.1–12.3.10): • Explicit approval from authorized parties to use the technologies. • All technology use to be authenticated with user ID and password or other authentication item. • A list of all devices and personnel authorized to use the devices. • A method to accurately and readily determine owner, contact information, and purpose. • Acceptable uses for the technology. • Acceptable network locations for the technology. • A list of company-approved products. • Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. • Activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. • Prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	*Int-1* *Int-2* *Int-3*					
12.3.1 Explicit approval by authorized parties.			☒	☐	☐	☐	☐
12.3.1 Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies.	**Provide the name of the assessor** who attests that the usage policies were verified to include processes for explicit approval from authorized parties to use the technologies.	*David M Dennis*					
12.3.2 Authentication for use of the technology.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.3.2 Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token).	**Provide the name of the assessor** who attests that the usage policies were verified to include processes for all technology use to be authenticated with user ID and password or other authentication item.	*David M Dennis*					
12.3.3 A list of all such devices and personnel with access.			☒	☐	☐	☐	☐
12.3.3 Verify that the usage policies define: • A list of all critical devices, and • A list of personnel authorized to use the devices.	**Provide the name of the assessor** who attests that the usage policies were verified to define: • A list of all critical devices, and • A list of personnel authorized to use the devices.	*David M Dennis*					
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).			☒	☐	☐	☐	☐
12.3.4 Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).	**Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine: • Owner • Contact Information • Purpose	*David M Dennis*					
12.3.5 Acceptable uses of the technology.			☒	☐	☐	☐	☐
12.3.5 Verify that the usage policies define acceptable uses for the technology.	**Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology.	*David M Dennis*					
12.3.6 Acceptable network locations for the technologies.			☒	☐	☐	☐	☐
12.3.6 Verify that the usage policies define acceptable network locations for the technology.	**Provide the name of the assessor** who attests that the usage policies were verified to define acceptable network locations for the technology.	*David M Dennis*					
12.3.7 List of company-approved products.			☒	☐	☐	☐	☐
12.3.7 Verify that the usage policies include a list of company-approved products.	**Provide the name of the assessor** who attests that the usage policies were verified to include a list of company-approved products.	*David M Dennis*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.			☒	☐	☐	☐	☐
12.3.8.a Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	**Provide the name of the assessor** who attests that the usage policies were verified to require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	*David M Dennis*					
12.3.8.b Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity.	**Identify** any remote access technologies in use	*OpenSSH* *FortiClient*					
	Describe how configurations for remote access technologies verified that remote access sessions will be automatically disconnected after a specific period of inactivity.	*I observed with Int-1 assistance that idle sessions for OpenSSH and FortiClient time out with a 15-minute idle interval and require authentication afterwards.*					
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.			☒	☐	☐	☐	☐
12.3.9 Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	**Provide the name of the assessor** who attests that the usage policies were verified to require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	*David M Dennis*					
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.			☒	☐	☐	☐	☐
12.3.10.a Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	**Provide the name of the assessor** who attests that the usage policies were verified to prohibit copying, moving or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	*David M Dennis*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	**Provide the name of the assessor** who attests that the usage policies were verified to require, for personnel with proper authorization, the protection of cardholder data in accordance with PCI DSS Requirements.	*David M Dennis*					
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.			☒	☐	☐	☐	☐
12.4.a Verify that information security policy and procedures clearly define information security responsibilities for all personnel.	**Identify the information security policy and procedures** reviewed to verify that they clearly define information security responsibilities for all personnel**.**	*Doc-1*					
12.4.b Interview a sample of responsible personnel to verify they understand the security policies.	**Identify the responsible personnel** interviewed for this testing procedure who confirm they understand the security policy.	*Int-1* *Int-2*					
12.4.1 ***Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management			☒	☐	☐	☐	☐
12.4.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance	**Identify the documentation** examined to verify that executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.	*Doc-1*					
12.4.1.b Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.	**Identify the company's PCI DSS charter** examined to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.	*Doc-1*					
12.5 Assign to an individual or team the following information security management responsibilities:			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.5 Examine information security policies and procedures to verify: • The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. • The following information security responsibilities are specifically and formally assigned:	**Identify the information security policies and procedures** reviewed to verify: • The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. • The following information security responsibilities are specifically and formally assigned:	*Doc-1*					
12.5.1 Establish, document, and distribute security policies and procedures.			☒	☐	☐	☐	☐
12.5.1 Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: • Establishing security policies and procedures. • Documenting security policies and procedures. • Distributing security policies and procedures.	*David M Dennis*					
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.			☒	☐	☐	☐	☐
12.5.2 Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: • Monitoring and analyzing security alerts. • Distributing information to appropriate information security and business unit management personnel.	*David M Dennis*					
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.5.3 Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: • Establishing security incident response and escalation procedures. • Documenting security incident response and escalation procedures. • Distributing security incident response and escalation procedures.	*David M Dennis*					
12.5.4 Administer user accounts, including additions, deletions, and modifications.			☒	☐	☐	☐	☐
12.5.4 Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for administering user account and authentication management.	*David M Dennis*					
12.5.5 Monitor and control all access to data.			☒	☐	☐	☐	☐
12.5.5 Verify that responsibility for monitoring and controlling all access to data is formally assigned.	**Provide the name of the assessor** who attests that responsibilities were verified to be formally assigned for: • Monitoring all access to data • Controlling all access to data	*David M Dennis*					
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.			☒	☐	☐	☐	☐
12.6.a Review the security awareness program to verify it provides awareness to all personnel about the cardholder data security policy and procedures.	**Provide the name of the assessor** who attests that the security awareness program was verified to provide awareness to all personnel about the cardholder data security policy and procedures.	*David M Dennis*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.6.b Examine security awareness program procedures and documentation and perform the following:	**Identify the documented security awareness program procedures and additional documentation** examined to verify that: • The security awareness program provides multiple methods of communicating awareness and educating personnel. • Personnel attend security awareness training: – Upon hire, and – At least annually • Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy.	*Doc-1* *Doc-5*					
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*			☒	☐	☐	☐	☐
12.6.1.a Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions).	**Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel.	*I observed during live remote Zoom meeting with Int-1 and Int-8 that Sangoma uses CPNI training from FCC and other sites for its security awareness training. I observed that Clearstar is used to manage the documents which are then reviewed by employees. I observed that Echosign is used to digitally sign the document copy given to employees (Doc-5).*					
12.6.1.b Verify that personnel attend security awareness training upon hire and at least annually.	**Describe how** it was observed that all personnel attend security awareness training:						
	• Upon hire	*I observed during live Zoom session interview with Int-8 that It is an onboarding step for employees to be training in job-relevant and general best practices security as they apply to Sangoma.*					
	• At least annually	*I observed tracking by Sangoma on internal Clearstar site during live remote Zoom meeting with Int-1 and Int-8. I was provided with Sample Set-21, which is used by Int-1 to confirm the results of training.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.6.1.c Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security.	**Identify the sample** of personnel interviewed for this testing procedure..	*Int-3* *Int-4* *Int-5* *Int-7* *Int-8*					
	For the interview, **summarize the relevant details** discussed that verify they have completed awareness training and are aware of the importance of cardholder data security.	*I verified by interview with Int-8 that Sangoma employees are taught to never handle cardholder data, as part of Sangoma' business model. Sangoma treats all data as high importance in the production network.*					
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.			☒	☐	☐	☐	☐
12.6.2 Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.	**Describe how** it was observed that, per the security awareness program, all personnel:						
	• Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic).	*I reviewed during live Zoom remote session that Employees sign an acknowledgement upon hire of understanding security as it applies to their roles for Sangoma. I observed printed copies of Doc-5 final page of the policy, where the employee had signed the document.*					
	• Provide an acknowledgement at least annually.	*I learned by interview with Int-1 and Int-8 that employees must take a security refresh course and test results are tracked annually.*					
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.7 Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	**Identify the Human Resources personnel** interviewed who confirm background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	*Int-8*					
	Describe how it was observed that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	*I observed by interview with Int-1 and Int-8 by remote Zoom session. I was told by Int-1 that Sangoma has no cardholder data in its possession and no employees that handle cardholder data. I was told by Int-8 that criminal background checks are performed on all new hires.*					
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:			☒	☐	☐	☐	☐
12.8 Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows:	**Identify the documented policies and procedures** reviewed to verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, per 12.8.1–12.8.5:	*Doc-1* *Doc-6* *Doc-14*					
12.8.1 Maintain a list of service providers including a description of the service provided.			☒	☐	☐	☐	☐
12.8.1 Verify that a list of service providers is maintained and includes a list of the services provided.	**Describe how** the documented list of service providers was observed to be maintained (kept up-to-date) and includes a list of the services provided.	*I observed that Sangoma maintains a list of service providers in Doc-14 that it uses, which consists of upstream co-located data centers (Sample Set-16 and Sample Set-18) which includes services provided.*					
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's CDE. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.8.2 Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	**Describe how** written agreements for each service provider were observed to include an acknowledgement by service providers that they will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.	*During the interview with Int-1, I observed examples that there are agreements in place as part of Doc-14 that require Sample Set-16 to remain complaint, and for Sangoma to track this compliance, either by AoC or by manual review of the site.*					
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.			☒	☐	☐	☐	☐
12.8.3 Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider.	**Identify the policies and procedures** reviewed to verify that processes included proper due diligence prior to engaging any service provider.	*Doc-1* *Doc-6* *Doc-14*					
	Describe how it was observed that the above policies and procedures are implemented.	*I interviewed Int-1, who stated that Sangoma policy requires that diligence for service provider compliance be performed. I reviewed Doc-14 and found this matched policy. This policy is used to review providers found in Doc-14 and Sample Set-16.*					
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.			☒	☐	☐	☐	☐
12.8.4 Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	**Describe how** it was observed that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	*I observed in Doc-14 that Sangoma policy requires compliance status monitoring by Sangoma throughout the year, with updates to compliance tracking occurring annually.*					
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.			☒	☐	☐	☐	☐
12.8.5 Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**Describe how** it was observed that the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	*Artifacts tracked in Doc-14 are provided by Sample Set-16 to confirm which requirements they are responsible for. Sangoma maintains its own list of responsibilities in Doc-1. I observed both documents and confirmed this status is kept up to date.*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.9 ***Additional requirement for service providers only*****:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*			☒	☐	☐	☐	☐
12.9 ***Additional testing procedure for service provider assessments only****:* Review service provider's policies and procedures and observe templates used for written agreement to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	**Indicate whether** the assessed entity is a service provider. **(yes/no)** *If "no," mark the remainder of 12.9 as "Not Applicable."* *If "yes":*	*yes*					
	Identify the service provider's policies and procedures reviewed to verify that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	*Doc-6* *Doc-14* *Doc-30* *Doc-41*					
	Describe how the templates used for written agreement verified that the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	*I read Doc-6 which describes how customer connectivity is set up at Sangoma using templates. I read Doc-14 to observe Sangoma is tracking service providers and what requirements are met by them in data centers. I read Doc-41 to learn there is a check-box "turn-up procedure" template used for all customer onboarding into the network, and that these include PCI-aligned requirements being met by configurations which must be in place and are checked. I read Doc-30 to observe which requirements are met by Sangoma, which are met by customers, and which are shared. I interviewed Int-1, Int-2 and Int-3 to confirm these procedures were followed. These led to a determination of compliance.*					
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.10 Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following:	**Identify the documented incident response plan and related procedures** examined to verify the entity is prepared to respond immediately to a system breach, with defined processes as follows from 12.10.1–12.10.6: • Create the incident response plan to be implemented in the event of system breach. • Test the plan at least annually. • Designate specific personnel to be available on a 24/7 basis to respond to alerts: – 24/7 incident monitoring – 24/7 incident response • Provide appropriate training to staff with security breach response responsibilities. • Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. • Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	*Doc-53*					
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. • Specific incident response procedures. • Business recovery and continuity procedures. • Data back-up processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.10.1.a Verify that the incident response plan includes: • Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. • Specific incident response procedures. • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). • Coverage and responses for all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	**Provide the name of the assessor** who attests that the incident response plan was verified to include: • Roles and responsibilities. • Communication strategies. • Requirement for notification of the payment brands. • Specific incident response procedures. • Business recovery and continuity procedures. • Data back-up processes. • Analysis of legal requirements for reporting compromises. • Coverage for all critical system components. • Responses for all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	*David M Dennis*					
12.10.1.b Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.	**Identify the responsible personnel** interviewed who confirm that the documented incident response plan and procedures are followed.	*Int-1* *Int-2*					
	Identify the sample of previously reported incidents or alerts selected for this testing procedure.	*Sample Set-3*					
	For each item in the sample, **describe how** the documented incident response plan and procedures were observed to be followed.	*I read the reported incident and compared it to Doc-23 and found that the major points in the process were accounted for in the report.*					
12.10.2 Review and test the plan at least annually, including all elements listed in Requirement 12.10.1.			☒	☐	☐	☐	☐
12.10.2 Interview personnel and review documentation from testing to verify that the plan is tested at least annually and	**Identify the responsible personnel** interviewed who confirm that the incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1.	*Int-1*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
that testing includes all elements listed in Requirement 12.10.1.	**Identify documentation** reviewed from testing to verify that the incident response plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1.	*Doc-23*					
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.			☒	☐	☐	☐	☐
12.10.3 Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	**Identify the document** requiring 24/7 incident response and monitoring coverage for: • Any evidence of unauthorized activity. • Detection of unauthorized wireless access points. • Critical IDS alerts. • Reports of unauthorized critical system or content file changes.	*Doc-23*					
	Identify the responsible personnel interviewed who confirm 24/7 incident response and monitoring coverage for: • Any evidence of unauthorized activity. • Detection of unauthorized wireless access points. • Critical IDS alerts. • Reports of unauthorized critical system or content file changes.	*Int-1* *Int-2* *Int-3* *Int-7*					
	Describe how it was observed that designated personnel are available for 24/7 incident response and monitoring coverage for: • Any evidence of unauthorized activity. • Detection of unauthorized wireless access points. • Critical IDS alerts. • Reports of unauthorized critical system or content file changes.	*I interviewed Int-1, Int-3 and Int-7 and read Doc-23 and observed that the Security group is available for incidents, as defined by the policy as well as seen during the incident table-top exercise. I interviewed Int-1, Int-2, Int-3 and Int-7 and read Doc-23 and observed that the Security group is notified when IDS alerts occur, by email sent to the Security group alias, which includes at a minimum Int-1, Int-2 and the TAC group. I interviewed Int-1, Int-2, Int-3 and Int-7 and read Doc-23 and observed that an OSSEC alarm will be emailed to the Security group any time an unauthorized file is placed into a monitored directory, this was demonstrated during live remote Zoom review.*					
12.10.4 Provide appropriate training to staff with security breach response responsibilities.			☒	☐	☐	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
12.10.4 Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained.	**Identify the responsible personnel** interviewed who confirm that staff with responsibilities for security breach response are periodically trained.	*Int-1*					
	Identify the documented policy reviewed to verify that staff with responsibilities for security breach response are periodically trained.	*Doc-1* *Doc-5* *Doc-23* *Sample Set-21*					
	Describe how it was observed that staff with responsibilities for security breach response are periodically trained.	*I observed during live Zoom review the annual training exercise tracking from 19, Jan 2024, in Sample Set-21 which included test scores of all personnel who were enrolled.*					
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.			☒	☐	☐	☐	☐
12.10.5 Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan.	**Describe how** processes were reviewed to verify that ***monitoring*** alerts from security monitoring systems are covered in the Incident Response Plan.	*I observed in Doc-18 that an alert which was received was among those listed by incident response plan in Doc-17.*					
	Describe how processes were reviewed to verify that ***responding to*** alerts from security monitoring systems are covered in the Incident Response Plan.	*I observed by the follow-up log in Doc-23 that incidents were responded to by authorized personnel. This was covered by the procedure in Doc-17.*					
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			☒	☐	☐	☐	☐
12.10.6 Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan: • According to lessons learned. • To incorporate industry developments.	*Doc-1* *Doc-23*					
	Identify the responsible personnel interviewed who confirm that processes are implemented to modify and evolve the incident response plan: • According to lessons learned. • To incorporate industry developments.	*Int-1* *Int-2*					
	Describe how it was observed that processes are implemented to modify and evolve the incident response plan:						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	• According to lessons learned.	*Int-1 described the process of post-mortem that occurs on incidents and also after their table top exercise. If the incident that occurred was found to impact existing policy, then policy was modified to reflect the evolved scenario according to lessons learned from the incident. There were no incidents that fit this description in 2023-2024, however, it was under policy to do so if that had been the case.*					
	• To incorporate industry developments.	*Int-1 described that he and the others tasked with security keep up with industry developments by reading security web sites and subscribing to several feeds of security news. This knowledge is then available for use with their risk assessment activities and as lessons-learned review after incident.*					
12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes			☒	☐	☐	☐	☐
12.11.a Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	**Identify the policies and procedures** examined to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	*Doc-1*					
12.11.b Interview responsible personnel and examine records of reviews to verify	**Identify the document(s) related to reviews** examined to verify that reviews are performed at least quarterly.	*Doc-19*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
that reviews are performed at least quarterly	**Identify the responsible personnel** interviewed who confirm that reviews are performed at least quarterly	*Int-1*					
12.11.1 ***Additional requirement for service providers only*****:** Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program			☒	☐	☐	☐	☐
12.11.1.a Examine documentation from the quarterly reviews to verify they include: • Documenting results of the reviews. • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program.	**Identify the document(s) related to quarterly reviews** to verify they include: • Documenting results of the reviews. • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program.	*Doc-19*					

Appendix A: Additional PCI DSS Requirements

This appendix contains additional PCI DSS requirements for different types of entities. The sections within this Appendix include:

- Appendix A1 Additional PCI DSS Requirements for Shared Hosting Providers
- Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI terminal connections
- Appendix A3: Designated Entities Supplemental Validation

Guidance and applicability information is provided within each section.

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

Note: *If the entity is not a shared hosting provider (and the answer at 2.6 was "no," indicate the below as "Not Applicable." Otherwise, complete the below.*

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
Indicate whether the assessed entity is a shared hosting provider (indicated at Requirement 2.6). **(yes/no)** *If "no,"* mark the below as "Not Applicable" (no further explanation required) *If "yes,"* ***complete the following:***			*no*				
A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*							
A1 Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A1.1 through A1.4 below:							
A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.			☐	☐	☒	☐	☐
A1.1 If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID.	**Indicate whether** the hosting provider allows hosted entities to run their own applications. **(yes/no)**	*no*					
	If "no":						
	Describe how it was observed that hosted entities are not able to run their own applications.						
	Not Applicable						
	If "yes":						
	Identify the sample of servers selected for this testing procedure.	*Not Applicable*					

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Identify the sample of hosted merchants and service providers (hosted entities) selected for this testing procedure.	*Not Applicable*					
• All CGI scripts used by an entity must be created and run as the entity's unique user ID.	*For each item in the sample,* **describe how** the system configurations verified that all hosted entities' application processes are run using the unique ID of that entity.						
	Not Applicable						
	Describe how the hosted entities' application processes were observed to be running using the unique ID of the entity.						
	Not Applicable						
A1.2 Restrict each entity's access and privileges to its own cardholder data environment only.			☐	☐	☒	☐	☐
A1.2.a Verify the user ID of any application process is not a privileged user (root/admin).	*For each item in the sample of servers and hosted entities from A1.1, perform the following:*						
	Describe how the system configurations verified that user IDs for hosted entities' application processes are not privileged users.						
	Not Applicable						
	Describe how running application process IDs were observed to verify that the process IDs are not privileged users.						
	Not Applicable						
A1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) ***Important:*** *An entity's files may not be shared by group.*	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** the system configuration settings verified:						
	– Read permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files.						
	Not Applicable						
	– Write permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files.						
	Not Applicable						
	– Access permissions are only assigned for the files and directories the hosted entity owns, or for necessary systems files.						
	Not Applicable						
A1.2.c Verify that an entity's users do not have write access to shared system binaries.	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** the system configuration settings verified that an entity's users do not have write access to shared system binaries.						
	Not Applicable						
A1.2.d Verify that viewing of log entries is restricted to the owning entity.	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** the system configuration settings verified that viewing of log entries is restricted to the owning entity.						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
	Not Applicable						
A1.2.e *To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources:* • Disk space • Bandwidth • Memory • CPU	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** the system configuration settings verified restrictions are in place for the use of:						
	• Disk space						
	Not Applicable						
	• Bandwidth						
	Not Applicable						
	• Memory						
	Not Applicable						
	• CPU						
	Not Applicable						
A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.			☐	☐	☒	☐	☐
A1.3 Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review by the owning entity. • Log locations are clearly communicated to the owning entity.	*For each item in the sample of servers and hosted entities from A1.1,* **describe how** processes were observed to verify the following:						
	• Logs are enabled for common third-party applications.						
	Not Applicable						
	• Logs are active by default.						
	Not Applicable						
	• Logs are available for review by the owning entity.						
	Not Applicable						
	• Log locations are clearly communicated to the owning entity.						
	Not Applicable						

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.			☐	☐	☒	☐	☐
A1.4 Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.	**Identify the document** examined to verify that written policies provide for a timely forensics investigation of related servers in the event of a compromise.	*Not Applicable*					

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

Entities using SSL and early TLS for POS POI terminal connections must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment terminals. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

The PCI DSS requirements directly affected are:

Requirement 2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
Requirement 2.3	Encrypt all non-console administrative access using strong cryptography.
Requirement 4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

SSL and early TLS must not be used as a security control to meet these requirements, except in the case of POS POI terminal connections as detailed in this appendix. To support entities working to migrate away from SSL/early TLS on POS POI terminals, the following provisions are included:

- New POS POI terminal implementations must not use SSL or early TLS as a security control
- All POS POI terminal service providers must provide a secure service offering**.**
- Service providers supporting existing POS POI terminal implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals in card-present environments that can be verified as not being susceptible to any known exploits for SSL and early TLS, **and the SSL/TLS termination points to which they connect,** may continue using SSL/early TLS as a security control.

This Appendix only applies to entities using SSL/early TLS as a security control to protect POS POI terminals, including service providers who provide connections into POS POI terminals.

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
Indicate whether the assessed entity is using SSL / early TLS for POS POI terminal connections. **(yes/no)** *If "no,"* mark the below as "Not Applicable" (no further explanation required) *If "yes,"* ***complete the following (as applicable):***			*no*				
A2.1 Where POS POI terminals (at the merchant or payment acceptance location) use SSL and/or early TLS, the entity must confirm the devices are not susceptible to any known exploits for those protocols. ***Note:*** *This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.*			☐	☐	☒	☐	☐
A2.1 *For POS POI terminals using SSL and/or early TLS,* confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	**Identify the documentation** examined to verify that the POS POI terminals using SSL and/or early TLS are **not** susceptible to any known exploits for SSL/early TLS.	*Not Applicable*					
A2.2 ***Requirement for Service Providers Only:*** All service providers with existing connection points to POS POI terminals referred to in A2.1 that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.			☐	☐	☒	☐	☐

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
A2.2 Review the documented Risk Mitigation and Migration Plan to verify it includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; • Risk-assessment results and risk-reduction controls in place; • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; • Overview of migration project plan to replace SSL/early TLS at a future date.	**Identify the documented Risk Mitigation and Migration Plan** reviewed to verify it includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; • Risk-assessment results and risk-reduction controls in place; • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; • Overview of migration project plan to replace SSL/early TLS at a future date.	*Not Applicable*					
A2.3 ***Requirement for Service Providers Only:*** All service providers must provide a secure service offering.			☐	☐	☒	☐	☐
A2.3 Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for their service.	**Identify the supporting documentation** reviewed to verify the service provider offers a secure protocol option for their service	*Not Applicable*					
	Identify the sample of system components examined for this testing procedure.	*Not Applicable*					
	For each item in the sample, **describe how** system configurations verify that the service provider offers a secure protocol option for their service.	*Not Applicable*					

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities that are required to validate to these requirements should refer to the following documents for reporting:

- *Reporting Template for use with the PCI DSS Designated Entities Supplemental Validation*
- *Supplemental Attestation of Compliance for Onsite Assessments – Designated Entities*

These documents are available in the PCI SSC Document Library.

Note that an entity is ONLY required to undergo an assessment according to this Appendix if instructed to do so by an acquirer or a payment brand.

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Guidance Column* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

   Note: *The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.*

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review.

   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) one-time passwords.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

***Note:** Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

Information Required		Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Not Applicable*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*Not Applicable*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Not Applicable*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Not Applicable*
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Not Applicable*
6. Maintenance	Define process and controls in place to maintain compensating controls.	*Not Applicable*

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement noted as being "in place" via compensating controls.

Requirement Number: *8.1.1 – Are all users identified with a unique user ID before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers using their regular user accounts, and then use the "sudo" command to run any administrative commands. This allows use of the "root" account privileges to run pre-defined commands that are recorded by sudo in the security log. In this way, each user's actions can be traced to an individual user account, without the "root" password being shared with the users.*
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the sudo command is configured properly using a "sudoers" file, that only pre-defined commands can be run by specified users, and that all activities performed by those individuals using sudo are logged to identify the individual performing actions using "root" privileges.*
6. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure sudo configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually identified, tracked and logged.*

Appendix D: Segmentation and Sampling of Business Facilities/System Components