System and Organization Controls (SOC) 2 Report on Controls Placed in Operation

Sangoma US, Inc.'s Description of its Cloud-based Business Communications Offerings Services System

For the Security and Availability Trust Services Criteria

As of May 31, 2024

Sangoma US, Inc.

SOC 2 Type I Report
As of May 31, 2024

TABLE OF CONTENTS

Independent Service Auditor's Report

To the Management of Sangoma US, Inc.:

Scope

We have examined Sangoma US, Inc.'s ("Sangoma") accompanying description of its Cloud-based Business Communications Offerings Services titled "Sangoma US, Inc.'s Description of its Cloud-based Business Communications Offerings Services System" as of May 31, 2024, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design of controls stated in the description as of May 31, 2024, to provide reasonable assurance that Sangoma's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Sangoma uses subservice organizations for services relating to colocation and cloud back up services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Sangoma, to achieve Sangoma's service commitments and system requirements based on the applicable trust services criteria. The description presents Sangoma's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sangoma's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Sangoma, to achieve Sangoma's service commitments and system requirements based on the applicable trust services criteria. The description presents Sangoma's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Sangoma's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Sangoma is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Sangoma's service commitments and system requirements were achieved. Sangoma has provided the accompanying assertion titled "Management of Sangoma US, Inc.'s Assertion Regarding its Cloud-based Business Communications Offerings Services System" (assertion) about the description and the suitability of the design of controls stated therein. Sangoma is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description; selecting the applicable trust services criteria and stating the related controls in the description and identifying the risks that threaten the achievement of Sangoma's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. the description presents Sangoma US, Inc.'s Description of its Cloud-based Business Communications Offerings Services System that was designed and implemented as of May 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of May 31, 2024 to provide reasonable assurance that Sangoma's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Sangoma's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Sangoma, user entities of Sangoma US, Inc.'s Description of its Cloud-based Business Communications Offerings Services System as of May 31, 2024, business partners of Sangoma subject to risks arising from interactions with the Cloud-based Business Communications Offerings Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organizations' systems interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Young & Associates, LLP

August 23, 2024
Lakewood, CO

SECTION TWO: Management of Sangoma US, Inc.'s Assertion Regarding its Cloud-based Business Communications Offerings Services System

We have prepared the accompanying description titled "Sangoma US, Inc.'s Description of its Cloud-based Business Communications Offerings Services System" ("description") for the as of date May 31, 2024 based on the criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) ("description criteria"). The description is intended to provide report users with information about the Cloud-based Business Communications Offerings Services System ("System") that may be useful when assessing the risks arising from interactions with Sangoma US, Inc.'s ("Sangoma") System, particularly information about system controls that Sangoma has designed to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria").

Sangoma uses a subservice organization to provide services relating to colocation and data backup storage services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Sangoma, to achieve Sangoma's service commitments and system requirements based on the applicable trust services criteria. The description presents Sangoma's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sangoma's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Sangoma, to achieve Sangoma's service commitments and system requirements based on the applicable trust services criteria. The description presents Sangoma's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Sangoma controls.

We confirm to the best of our knowledge that:

a. the description presents Sangoma US, Inc.'s Cloud-based Business Communications Offerings Services System that was designed as of May 31, 2024, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of May 31, 2024 to provide reasonable assurance that Sangoma US, Inc. service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Sangoma US, Inc.'s controls as of that date.

Eric Krichbaum
Chief Information Security Officer

August 23, 2024

SECTION THREE: Sangoma US, Inc.'s Description of its Cloud-based Business Communications Offerings Services System

Overview of Operations

Background

Sangoma US, Inc. ("Sangoma") is a leading global Communications as a Service (CaaS) provider empowering businesses of all sizes to connect to the people and processes that matter. Sangoma is a rapidly growing, profitable, customer-centric company with an installed base of over 2.5 million Unifed Communications seats. Sangoma has been recognized as a trusted leader in the communications industry and offers a stable, global presence and a diverse portfolio of solutions, services, and support.

Services Overview

Sangoma offers a suite of Cloud-native Communications solutions. Sangoma's cloud-based business communication services include Unified Communication, Video Meetings, Collaboration, Apps, Trunking, Fax, Network, and Security offerings that include:

- **Video Meetings as a Service (MaaS) -** Sangoma's MaaS solution, Sangoma Meet, is a secure, meet-from-anywhere video meetings and collaboration platform that you can leverage from any internet-connected device. Sangoma Meet enables file sharing on screen, integrates seamlessly with your calendar, supports PSTN dial-in, offers virtual backgrounds, simplifies attendee management from within and outside of the organization, and many other key features. MaaS allows businesses to maintain an in-office meeting experience while working remotely and including attendees from anywhere, seamlessly.

- **Contact Center as a Service (CCaaS) -** Sangoma's CCaaS solutions are designed to optimize customer engagement through advanced inbound and departmental service features.

- **Communications Platform as a Service (CPaaS) –** Sangoma's CPaaS implementation features integration and customization to support one's unique workflows. The system provides a common business backbone for remaining connected with users and processes, and extends elements for blending communications with sales, marketing, e-commerce, finance and customer relationship management aspects. Among the service's main selling points are custom workflows, integrations and development options, as well as support for end-to-end communications and on-demand access to Sangoma professional services.

- **Managed Security Services** - Sangoma's managed security services provide comprehensive protection against a wide range of cyber threats, crucial for maintaining a secure IT environment.

- **Managed Internet and SD-WAN Services** - These services offer secure and reliable network solutions tailored to the needs of modern businesses, ensuring connectivity and performance.

- **Devices as a Service (DaaS) -** Sangoma's DaaS solution provides a suite of integrated hardware solutions, including phones, headsets, and network connectivity equipment.

- **Fax as a Service (FaaS)** - FAXStation, Sangoma's FaaS solution, provides modern and reliable faxing capabilities.

- **Trunking as a Service (TaaS)** - SIP trunks allow businesses to continue leveraging their existing communications infrastructure while also upgrading their service to the cloud. Sangoma's TaaS solutions deliver internet-based telephony services via the customer's existing internet connection, helping them save money and elevate their communications with access to our leading Unified Communication as a Service "CaaS" portfolio.

Sangoma customers exist in many different vertical markets and vary greatly in size. A typical customer would have 1 to 3 services typically, possibly including managed circuits, wan connectivity and voice (physical phone or softphone).

With offices in many cities around the world, Sangoma is a diverse group of cultures and individuals providing our customers with these varied services.

- Corporate HQ – Markham, ON, Canada
- United States HQ - Sarasota FL, US
- Huntsville AL, US
- Atlanta GA, US
- Parsippany NJ, US
- Amherst NY, US
- Pittsburgh PA, US
- Sydney NSW, Australia
- New Delhi, India
- Bangalore Karnataka, India
- Manila, Philippines
- Envigado Antioquia, Colombia
- Wokingham, United Kingdom
- München, Germany

Scope

This report describes the control structure of Sangoma as it relates to the system, internal IT infrastructure, related software, and processes to support the Trust Services Criteria for Security and Availability. The description is intended to provide information regarding the design of the controls listed herein and focus on the components listed below:

- Infrastructure — The facilities, equipment, and network;
- Software — The systems, applications, and utilities;
- People — The developers, administrators, users, and managers;
- Procedures — The automated and manual procedures involved in the operation of the system, and;
- Data — The transaction streams, files, databases, and tables used to support the system.

This report is intended to focus on features relevant to specific controls; it does not encompass all aspects of the procedures followed by Sangoma. If a user organization does not have an effective internal control structure in place, the controls and related Trust Services Criteria presented in this report may not compensate for such a weakness.

Service Commitments and System Requirements

Sangoma's service commitments and system requirements include a secure environment for the data stored and processed by the system. Sangoma's commitments include:

- Ensuring the continued security of customer data and the Sangoma systems;
- Ensuring computing systems are maintained and up to date with security patches;
- Ensuring duties are properly segregated through the development and deployment processes;
- Ensuring that staff are properly trained on information security policies and procedures, and;
- Ensuring access levels to information is monitored and that access is only granted to individuals who require access to perform their job.

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements as of this report.

Sangoma has developed and implemented a complete Incident Response policy and plan that includes the following steps of the Incident Response Process:

- Detection, Classification, and Type Determination
- Containment and Evidence Collection
- Eradication and Notification
- Recovery
- Evaluation, Lessons Learned, Root Cause Analysis, and Root Cause Remediation.

Sangoma documents and tracks detected incidents in its workflow management system to ensure root causes are determined and controls, which may have been designed inadequately or operating ineffectively are reviewed and enhanced as necessary.

Subservice Organizations

Sangoma utilizes a subservice organizations, as described below, to provide its Cloud-based Business Communications Offerings Services System services to its customers. The description included in Section Three of this report does not include a detailed description of these organizations, and they have been excluded from this report under the carve-out method.

Sangoma utilized the carve-out method because it believes it can perform adequate monitoring procedures of the controls performed at the subservice locations, including the review of subservice organizations' Service Organization Control reports and other monitoring procedures.

Subservice Organization	Services Provided
Physical Third-Party Datacenters	
CoreSite – Physical infrastructure being hosted at the following datacenter(s) locations:: Chicago, IL; Reston, VA; Los Angeles, CA; Atlanta, GA; Denver, CO	These third-party datacenters provide co-location hosting space and physical security. Sangoma manages the logical access to the co-location third-party data center for production systems and data. Sangoma has limited physical access to these data centers and utilizes the datacenters for all physical access controls to the co-location third-party data center.
Equinix – Physical infrastructure being hosted at the following datacenter(s) locations: Chicago, IL; Sydney, Australia; Toronto, Canada	
Digital Realty – Physical infrastructure being hosted at the following datacenter(s) locations: Atlanta, GA; New York, NY; Clifton, NJ; Dallas, TX; San Francisco, CA; Marseille, France	
Lunavi – Physical infrastructure being hosted at the following datacenter(s) locations: Seattle, WA	
Crown Castle – Physical infrastructure being hosted at the following datacenter(s) locations: Los Angeles, CA	
Databank – Physical infrastructure being hosted at the following datacenter(s) locations: Dallas, TX	
Switch – Physical infrastructure being hosted at the following datacenter(s) locations: Las Vegas, NV	
365 Datacenters – Physical infrastructure being hosted at the following datacenter(s) locations: Reston, VA	
Cloud Provided Datacenter	
Amazon AWS	Sangoma uses AWS for cloud computing services and back-ups. AWS provides all the infrastructure resources, including hardware and bandwidth to support these system components. Sangoma manages logical access to these systems. Sangoma has no physical access to hardware at any of the AWS data centers.

Additional information regarding the subservice organizations is included in the Monitoring section of this report.

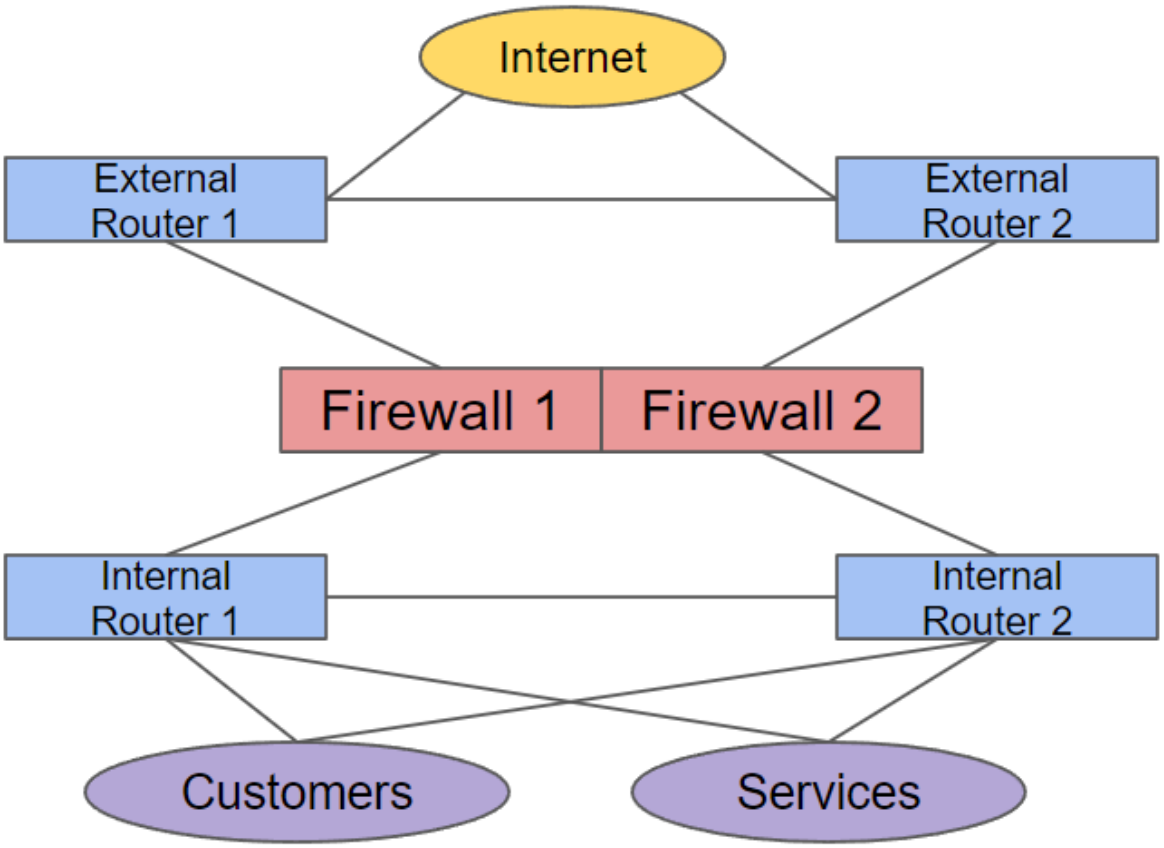
Components of the System

Infrastructure

Sangoma's information systems consist of facilities, computers, mobile devices, storage systems, and networking communication equipment in corporate infrastructure that is located within Sangoma's corporate headquarters located in Markham, Ontario, Canada and Sarasota, Florida.

A typical network point of presence offers a redundant connectivity design for customers and services. This reduces the impact of maintenance activity and provides for more robust availability. These network pops are hosted in third party datacenters using hardware and software from multiple vendors primarily based on Linux operating systems.

The Sangoma infrastructure is built to provide a highly available platform through equipment and service redundancy. Devices exist in an active/active or a hot standby (active/passive) configuration based on manufacturer abilities. This allows for a smooth transition of redundant services from any piece of gear for maintenance or failure events. Services that are single homed to a single specific device can achieve redundancy through other methods in the same or alternate data centers.



Software

Key Applications

Applications	Business Process/Function
Sangoma Internally Developed Software	
Meet	Video Conferencing
Teamhub	Chat and Collaboration
Community, Business Voice, Switchvox	Voice Services
Operating Systems	
Linux	Server Operating System
Windows	Desktop/Laptop/Server Operating System
MacOS	Desktop/Laptop Operating System
Purchased Software	
Arbor Sightline	Denial of Service Attack detection and mitigation
VMWare Velocloud	SDWan system
FortiEMS, FortiAuthenticator, FortiAV, FortiClient	Security services
Fortinet	Virtual DOMain (Segmentation technology)
Seceon	EDR and SIEM services
Rsyslog	Centralized Logging
BIND	Internal DNS (Domain Naming Services)
OpenSSH	Remote Access
OSSEC	HIDS / change-detection / FIM
Logwatch	Log Monitoring

Purchased Software (continued)	
ClamAV	Antivirus
Google authenticator plug-in	Multi-factor Authentication
Tenable Nessus	Internal Scan
Cisco TACACS	Authentication
Nagios	Monitoring Software
DNF and APT	Patch Management

People

Sangoma has implemented an organizational structure, which ensures the necessary independence, integrity, and reporting structures to support accounting and information technology general controls and environment. The implemented structure also ensures that duties are properly segregated between departments.

The following chart depicts Sangoma's organizational structure:

Groups/Teams	Function
Board of Directors	Strategic Direction and Oversight, Establishing Company Philosophy, Values, and Mission
Board Committees	Audit Committee, Compensation Committee, Nominating & Governance Committee
Chief Executive Officer	Direction in the company and strategic planning
Executive Officers	Establishing, Directing, and Managing company operations and for establishing, communicating, and monitoring internal controls, policies, and procedures
Executive Risk Committee	Implementing and monitoring compliance with applicable laws, regulations, standards, and guidance related to Information Security
Security Team	Designing and implementing security controls, Investigation of incidents, Notifying and Reporting of security incidents, Coordinating remediation efforts Monitoring and maintenance of systems, Interaction with customer and team issues related to the secure operation of infrastructure and products
Operations	Monitoring and maintenance of systems, Interaction with customer and team issues related to the secure operation of infrastructure and products
IT	Cloud and premised based back-office systems such as ERP, and CRM Maintaining and coordinating continued relationship with critical vendors.
Product	Marketing and customer vision. Product development and roadmap
Development	Implementation of Product goals. Test and validation of code.
People and Talent	Human Resource based functions such as onboarding and offboarding of staff and contractors.
Legal	Legal and Risk based functions

Procedures

Sangoma has implemented its Information Security Policies that are reviewed annually by the Information Security Committee for approval, over significant aspects of operations, which include:

a. security requirements for authorized users;
b. data classification and associated protection, access rights, retention and destruction requirements;
c. risk assessment;
d. access protection requirements;
e. user provisioning and deprovisioning;
f. responsibility and accountability for security;
g. responsibility and accountability for system changes and maintenance;
h. change management;
i. security and other incidents identification, response and mitigation;
j. security training; and,
k. information sharing and disclosure.

List of Policies & Guidelines

Policies & Guidelines	Business Process/Function
Cybersecurity Policy	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.
Information Protection Policy	The purpose of this policy is to establish security policies, processes, and procedures that shall be maintained and used to manage protection of information systems and assets.
Data Security Policy	The purpose of this policy is to establish the Confidentiality, Integrity, and Availability of all its data at rest, data in transit and data in use within systems in the network.
Asset Management Policy	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.
Business Environment Policy	The purpose of this policy is to establish requirements to ensure protection of the Company's supply chain that is accessible by employees and suppliers.
Firewall Policy	The purpose of this policy is to establish requirements to secure and protect the information assets owned by the Company. The Company provides computer devices, networks, and other electronic information systems to meet its missions, goals, and initiatives.
Access Control Policy	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.
Linux Server Guidelines	The purpose of this policy is to establish Linux server baseline security hardening guidelines.
Router Security Guidelines	The purpose of this policy is to establish the required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the Company.
Server Security Guideline	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.
Audit and Logging Policy	The purpose of this policy is to secure, log, monitor, and protect the information assets owned by the Company.
Incident Reporting Policy	The purpose of this policy is to establish the baseline incident response procedures and covers the response to and reporting of suspected or known security incidents.
Risk Management Policy	The purpose of this policy is to establish Risk Management and Vulnerability Management, and to establish requirements to ensure management of risk within the Company's technology that is accessible by employees, contractors and suppliers.
Wireless Communications Policy	This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to The Company network.

Policies(continued)	Business Process/Function
Business Continuity Policy	The purpose of this policy is to establish the Business Continuity Plan. This is to set the overall policy for each business unit to maintain operation during or after an event.
Firewall-Configuration-Standard-Template	The purpose of this template is to establish Sangoma's standard firewall FortiGate configuration. It contains the baseline security hardening required to meet security needs.
Security Monitoring Policy	The purpose of this policy is to establish the overall Sangoma Security Monitoring Policy for monitoring of availability and integrity of Sangoma systems and devices.
Breach Policy	The purpose of this policy is to establish the Sangoma Breach Policy for internal handling, reporting, and protecting evidence of a breach event.
Maintenance Policy	The purpose of this policy is to establish the overall "Company's" Maintenance Policy for internal handling of maintenance and serviceability of Sangoma systems and devices.
Protective Technology Policy	The purpose of this policy is to establish the overall "Company's" Protective Technology Policy such as audit logging, least privilege access, and physical and logical protections.
Security Awareness & Training Policy	The purpose of this policy is to establish the overall "Company's" Security Awareness & Training Policy to establish the requirements for ongoing training and updated information.
Recovery Planning Policy	The purpose of this policy is to establish the overall "Company's" Recovery Planning Policy for internal handling of recovery of service, operation, and/or necessary data after an event.
Whistleblower Policy	"Company's" Whistleblower Policy, is a public facing policy accessible on its website, and acknowledged by all employees. The Policy provides a mechanism report any concerns on a confidential and, if desired, anonymous basis to the "Company's" third-party confidential reporting system.
Third Party Policy	The purpose of this policy is to establish the overall "Company's" Third Party Policy for onboarding, offboarding, and maintain relations with third party companies.

Data

Data, as defined for Sangoma's in-scope systems, includes printed and electronic data or information submitted by its customers and users of the system. The data received includes customer information such as name, address, phone number, SSN, etc. to provide its Cloud-based Business Communications Offerings and Services .

The Sensitive Data Policy section in the Data Security Policy helps personnel determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Sangoma without proper authorization.

The Data Security Policy defines how encryption will be used. Per the Data Security Policy, Sangoma requires that data be encrypted when confidential information is in transit on a network or is stored on systems or devices.

Third-party Access

Logical access to Sangoma's systems is granted to third parties should they be contracted to provide support for Sangoma's system. Accounts are created at the beginning of the engagement and removed as soon as the contract for services has expired.

The third-party is granted access to the Sangoma system when work is being performed and the account is disabled when completed. Sangoma tracks when access is granted to the third-party within the ticketing system. Third parties accessing these systems are typically vendors performing work on systems that they maintain such as physical access to colocation facilities housing Sangoma equipment, or compute systems providing virtual machine and access services.

Boundary of the System

This report includes information about the infrastructure, software, people, procedures, and data required to deliver the Cloud-based Business Communications Offerings Services System to its customers and meet Sangoma's service commitments and system requirements.

Infrastructure, software, people, procedures, and data that only indirectly provide these services and the control activities at any subservice organization or user entity organization are not within the boundaries of the system.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring Controls

Sangoma's management has established a system of internal controls aligned with the integrated framework established by the Committee of Sponsoring Organizations (COSO). The following describes management's approach to addressing the various components of the COSO integrated framework.

Control Environment

Sangoma is committed to maintaining an organizational structure that supports an effective control environment. The control environment is comprised of various elements, including segregation of job duties, matching employee skill-sets with job functions, constant open communication between office personnel and management, management oversight, and significant checks and balances.

A Board of Directors has been implemented and operates under a Charter that outlines the responsibility to oversee the development and performance of the Company and which each member is required to acknowledge their understanding of their responsibility and review and approve at least annually. The Board of Directors operates under a charter that includes discussion of a business code of conduct that establishes ethical and integrity values which members are required to sign off acknowledging their understanding upon joining the board. The Board of Directors' Charter establishes the number of members, their qualifications, oversight responsibilities, at least two of its members be independent of management, required meeting frequencies, and background and skills of each member be reviewed upon invitation to join. Sangoma has implemented a Code of Business Conduct and Ethics which is reviewed and approved by the Board of Directors annually. The Board of Directors sets goals for performance and evaluation criteria including incentives, other rewards, and sanctions for the entire organization and reviews and approves those goals annually.

An Executive Risk Committee has been implemented and requires the committee to meet quarterly, record meeting minutes, be comprised of at least one member having security experience, and reports to the CEO/BoD on a quarterly basis.

Sangoma has an established organizational chart for the Company and job descriptions that include key considerations of authority and responsibility, as well as appropriate lines of reporting for key employees. The organizational chart is reviewed and approved by the CHRO at least annually. Job descriptions, outlining authority, roles and responsibility, are reviewed, approved, and maintained by People and Talent and are reviewed, updated, and approved by the hiring managers as needed. Job descriptions are reviewed by the employee and manager annually as part of the employees' performance evaluation. As part of the new hire and offer letter acceptance process, personnel agree to be verified against regulatory screening databases, including criminal checks and are reviewed by People and Talent. Based on the candidates' role, technical users of the system undergo a technical assessment as part of their onboarding and skill verification process.

People and Talent and the employees' manager review employees' performance annually to develop and align employees' goals with Sangoma's objectives. The employees and their managers both sign the performance review. Violations of the Code of Conduct are investigated timely and may result in disciplinary actions up to and including probation, suspension and termination of employment. Reports of significant cases will be summarized and presented to the CEO and CFO as needed. Internal users of the system are required to sign a Code of Conduct upon hire and annually thereafter that establishes integrity and ethical values and the consequences for violations.

People and Talent maintains a list of contractors that is reviewed on a quarterly basis to verify adherence to the Sangoma corporate governance documents and identify any contracts that have been completed. People and Talent and the employees' manager review employees' performance annually to develop and align employees' goals with Sangoma's objectives. The employees and their managers both sign the performance review.

The Security Team reports on identified deficiencies within internal controls, suggested remediations, and the appropriate control owner to the Operational Team Lead on a monthly basis that includes summaries of any completed third-party assessments of internal controls and automated vulnerability scans.

Upon onboarding of a High-Risk vendor and annually thereafter, the Security Committee reviews the formal service agreements and/or Terms of Service with High-Risk vendors to outline and document the security requirements that will be followed by each party. These commitments and each party's adherence to them will be reported to the Executive Risk Committee.

The Acceptable Use Policy outlines security standards for the use of electronic devices and network resources and sanctions for violations thereof which internal users are required to sign off on upon hire and annually thereafter.

Sangoma provides internal and external personnel with means to report ethics concerns and questions as noted within the Whistleblower Policy.

Risk Assessment

Sangoma performs an annual risk assessment to identify potential fraud threats that could impair system security, analyzes the significance of risks associated with the identified threats, and determines mitigation strategies for those risks. Identified risks are rated using a risk evaluation process and ratings reports are reviewed by the Security Team. The annual company-wide risk assessment identifies and assesses the following areas that could affect Sangoma's system of internal controls:

A. Assets and environment;
B. Business objectives and operations;
C. Financial strategies;
D. Vendors, business partners and direct and contract employees;
E. Regulatory changes;
F. Changes in the threat landscape;
G. Information technology;
H. Fraud risk, and;
I. Determining a risk mitigation strategy.

During the annual company-wide risk assessment, risks are identified as very low, low, moderate, high, or very high based on the likelihood of occurrence and measured based on the risk measurement criteria approved by the Security Team to evaluate the impact on the people, company assets, locational risks, assessment risks, financial risks, third party risks, fraud risks, regulatory risks, and fundamental principles of the organization. Sangoma performs a fraud risk assessment that identifies risks by assessing pressures, opportunities, attitudes and rationalizations of finance staff and to those in a position to influence them. All discovered risks that could impact security are entered into the risk register and assigned an owner depending on the risk type, tracked until resolved and approved by the Security Team documenting the risk has been mitigated. The Legal and Security Committee reviews client contracts that have material changes (amendments or changes) upon execution of the contract or when renewed for service commitments and system requirements and incorporates them into the annual risk assessment to identify risks that could impact them and develop mitigation strategies. The Executive Risk Committee meets quarterly to discuss strategy and operations, financial results, risk considerations and other factors critical to the business. The Security Team presents the annual company-wide risk assessment and management's mitigation strategies to the Executive Risk Committee. Business unit owners will follow their standard process for remediation, tracking, and approvals as needed.

Information and Communication

Information is the core of Sangoma’s processes and integrated systems. Sangoma maintains an information process that allows pertinent information and data to be identified, captured and communicated in a timely fashion enabling employees to efficiently fulfill their job responsibilities and functions. The information process utilizes data from both inside and outside the organization, which is used to guide Sangoma’s strategic and tactical decision making, as well as to measure performance.

Sangoma supports its Security Policies by designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system that is reviewed and approved by the Security Team on an annual basis and is available to all system users on the company's cloud share. Only the Infrastructure, Security, Legal, and Compliance Teams have access to make updates to these documents.

Internal users undergo annual security training and are required to confirm their understanding of and compliance with the security policies and the Acceptable Use Policy upon hire and annually thereafter. Job descriptions, outlining authority, roles and responsibility, are reviewed, approved, and maintained by People and Talent and are reviewed, updated, and approved by the hiring managers as needed. Job descriptions are reviewed by the employee and manager annually as part of the employees' performance evaluation. Sangoma's Security Incident Response Plan includes steps for timely identification, severity classification, investigation, reporting, and resolution of incidents, as well as communication to the affected parties. Identified or reported incidents are communicated to the appropriate teams and are tracked and logged through remediation in the ticketing system. The remediation results are communicated to Security and Legal Teams. The Security Team reports on identified deficiencies within internal controls, suggested remediations, and the appropriate control owner to the Operational Team Lead on a monthly basis that includes summaries of any completed third-party assessments of internal controls and automated vulnerability scans. The Security Team ensures that Sangoma's security commitments and system requirements are current by reviewing amendments or changes to client contracts and communicating changes to these requirements to the process owner of the control affected by the change. Sangoma communicates its security commitments to external users, with whom it shares information, through formal agreements. Sangoma communicates user security commitments, with whom it obtains information, through the Terms of Service or similar agreement based on product listed on the Company's website and as part of client contract.

The Security Team reviews the Description of Services as it relates to security on an annual basis. This Description of Services is communicated to appropriate business partners and clients via agreed upon means. Formal information sharing agreements are in place with High-Risk vendors. These agreements include security commitments applicable to that entity. Sangoma's Security Incident Response Plan includes steps for timely identification, severity classification, investigation, reporting, and resolution of incidents, as well as communication to the affected parties. Identified or reported incidents are communicated to the appropriate teams and are tracked and logged through remediation in the ticketing system. The remediation results are communicated to Security and Legal Teams. Sangoma maintains a list of complementary end user controls that are provided to the clients through its Terms of Service, which is included in its Subscription Agreement and is available on Sangoma's external website. Sangoma's users are alerted in the event of a security or maintenance-related issue via email and/or through its Trust Site.

The Executive Risk Committee formally approves controls which are evaluated and tested on an annual basis by a separate functional department from the process or control owner. The CISO reports the results of the internal audit to the Security Team on an annual basis, who reviews and approves the action plan prepared by management.

Monitoring

Sangoma management monitors internal processes and control effectiveness as part of routine operations. The monitoring functions are conducted by Sangoma management through a combination of assessment activities, continuous monitoring, and change management.

An internal audit, including an assessment of Sangoma's information security, is performed annually by the Security Team. Results from the internal audit are reported to management and the Executive Risk Committee. Sangoma has developed an internal audit process which requires a different member other than the process owner to validate internal controls on an annual basis. Results are documented, communicated, and tracked. Sangoma's internal audit program identifies process owners from all levels of management and includes a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment process.

Sangoma maintains a SIEM that aggregates and evaluates system logs to monitor network, database, server, and domain events to detect any unauthorized access. The logging system provides alerting based on rulesets identified by management, which is monitored by the Infrastructure and Security Teams via email when an event is triggered, and is used to: identify potential security threats, vulnerabilities, or breaches; and detect unusual system activity. The Security Team reviews security assessments and/or control attestation reports for in-scope vendors and subservice organizations during onboarding and annually thereafter to monitor for deficiencies that may introduce risk to Sangoma. Any findings and/or recommendations from the Security Team are documented and reviewed by the Security Steering Committee who will make recommendations to the Executive Risk Committee on how the risks will be mitigated.

Internal and external environments are scanned continually by the Security Team to identify security vulnerabilities. High and Critical vulnerabilities are reviewed during the weekly Security Team meeting and internal tickets or change controls are entered into the system for remediation in accordance with the Risk Management Policies. Sangoma engages with a third party to perform an external penetration test on the environment on a twice-annual basis, and the results are communicated to the Security Team. Any critical findings are remediated within 60 days. On a quarterly basis, an assessment is performed on the audit plan and scope of the audit to identify potential changes impacting Sangoma's risk profile and is presented to the Security Steering Committee. The Security Team reports on identified deficiencies within internal controls, suggested remediations, and the appropriate control owner to the Operational Team Lead on a monthly basis that includes summaries of any completed third-party assessments of internal controls and automated vulnerability scans. The Security Team monitors the corrective action plan on a monthly basis to verify deficiencies of internal controls are remediated on a timely basis.

Internal Audit

Sangoma has implemented a continuous scanning process in conjunction with its external audit. This process allows for peer review and reinforcement of practice within the organization. Asset management and vulnerability management tools allow for continual scanning of internal assets along with the mapping to operational and development owners for any remediation or compensating controls necessary to assess, mitigate, and remediate any security needs that may arise.

Sangoma has developed and implemented an internal audit process which requires a different member other than the process owner to validate internal controls on an annual basis. Results are documented, communicated, and tracked. Sangoma's internal audit program identifies process owners from all levels of management and includes a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment process. An internal audit, including an assessment of Sangoma's information security, is performed annually by the Security Team. Results from the internal audit are reported to management and the Executive Risk Committee. On a quarterly basis, an assessment is performed on the audit plan and scope of the audit to identify potential changes impacting Sangoma's risk profile and is presented to the Security Steering Committee. The CISO reports the results of the internal audit to the Security Team on an annual basis, who reviews and approves the action plan prepared by management.

Monitoring of Subservice Organization

Sangoma has implemented a Vendor Risk Management Program and policy to govern the monitoring of subservice organizations. Vendors are categorized by risk levels based on the criticality of the services provided to Sangoma and the sensitivity and / or volume of information they or their systems may have access to.

Vendor risk assessments are performed by the Compliance & Quality Assurance and Information Security Teams before engagement and annually for High-Risk vendors and subservice organizations with access to confidential data or the ability to affect the security of the system.

Information Technology Controls

Sangoma has implemented and operates logical and physical access controls to provide reasonable assurance that access to computer equipment, storage media and program documentation is restricted to properly authorized individuals.

Logical Access Controls

Sangoma's logical access controls are based on need to know, least privilege, and separation of duties. Role-Based Access Control is implemented through pre-defined group memberships with designated rights and permissions required by the identified role.

Predefined user groups are utilized to assign role-based access privileges to restrict authorized users' access. Network and application administration user accounts have been restricted to appropriate teams. Sangoma provides users with guidelines to keep their passwords secure which is documented in the Acceptable Use Policy.

The Access Control Policy requires minimum password complexity to be configured when accessing internal Sangoma systems. The Access Control Policy requires network accounts to be configured to be locked out after a limited number of unsuccessful login attempts and have the following minimum configuration:

- At least eight characters, and;
- Passwords must also contain 3 of the 4 of the following requirements:
  - Contain at least 8 alphanumeric characters;
  - Contain both upper- and lower-case letters;
  - Contain at least one number, and;
  - Contain at least one special character (e.g.: !@#$%^) in certain environments.

Access requests have a ticket opened and routed to the appropriate team to grant access based on role. Requests for additional access above the user's role to the system are made by the user and approved by the manager. Access requests are documented and tracked in Sangoma's internal ticketing system. A ticket is opened that tracks and notifies the appropriate teams when access has been revoked and network access is removed within 1 business day. This ticket is tracked through completion.

Sangoma requires multi-factor authentication ("MFA") to gain access to production application servers in the environment. Sangoma utilizes AES-256 encryption on all data stored at rest and in data backups. Backup access is limited to appropriate team.

The IT Team enables full disk encryption when issuing laptops to users. The Security Team performs quarterly reviews of the privileged user groups of the corporate network, and applications to verify that access is appropriate based on role to verify the role has the least required access for the job function. When internal or external users connect with in-scope systems; VPN, SSL/TLS, SSH, SFTP, or other transport encryption technologies are used for defined points of connectivity.

Sangoma maintains a SIEM that aggregates and evaluates system logs to monitor network, database, server, and domain events to detect any unauthorized access. The logging system provides alerting based on rulesets identified by management, which is monitored by the Infrastructure and Security Teams via email when an event is triggered, and is used to: identify potential security threats, vulnerabilities, or breaches; and detect unusual system activity. Sangoma employs locks, or other access control methods to physically secure its office locations to restrict access to authorized personnel only. Sangoma has implemented the Asset Management Policy which includes policies and procedures on the tracking of physical assets from purchase to destruction, requiring all assets capable of storing customer data obtain a certificate of destruction upon destruction of the asset.

Sangoma's network is segmented using subnets and VDOMs/VRFs/VPCs to restrict access and movement of data between segments to support isolation in event of a security incident and is reviewed annually by the Security Team. Sangoma's firewalls are restricted to the Security Team and are configured to limit unnecessary ports, protocols, and services which are reviewed monthly by the Security Team. Sangoma has an intrusion detection system ("IDS") to monitor Sangoma's network and the production environment by notifying the Security Team of potential security incidents. When internal or external users connect with in-scope systems; VPN, SSL/TLS, SSH, SFTP, or other transport encryption technologies are used for defined points of connectivity.

When email is sent from the system, the content of the messages and attachments are scanned to identify potential private data. The e-mail is encrypted in transit. When internal or external users connect with in-scope systems; VPN, SSL/TLS, SSH, SFTP, or other transport encryption technologies are used for defined points of connectivity.

The IT Team manages a corporate endpoint managed firewall solution on user computers and IT servers. Product Team maintains servers in the production product environments. Anti-virus software is deployed on all devices and is reviewed by the IT Team quarterly to ensure anti-virus software is up to date and operational. Sangoma scans all incoming and outgoing corporate emails for malicious software which, if found, is quarantined, and a notification is sent out based on incoming or outgoing destinations. Internal and external environments are scanned continually by the Security Team to identify security vulnerabilities. High and Critical vulnerabilities are reviewed during the weekly Security Team meeting and internal tickets or change controls are entered into the system for remediation in accordance with the Risk Management Policies.

Incident Response

The Security Team monitors the infrastructure and software using a device management system that measures compliance with company standards on an ongoing basis. Sangoma maintains a SIEM that aggregates and evaluates system logs to monitor network, database, server, and domain events to detect any unauthorized access. The logging system provides alerting based on rulesets identified by management, which is monitored by the Infrastructure and Security Teams via email when an event is triggered, and is used to: identify potential security threats, vulnerabilities, or breaches; and detect unusual system activity. Internal and external environments are scanned continually by the Security Team to identify security vulnerabilities. High and Critical vulnerabilities are reviewed during the weekly Security Team meeting and internal tickets or change controls are entered into the system for remediation in accordance with the Risk Management Policies. The Security Team uses software to scan for and apply operating system and application patches on Servers and Workstations. A member of the Security Team reviews patches monthly and releases appropriate patches following the change management procedures. Exceptions are noted in the ticketing system.

The Security Team meets monthly to review vulnerability scans, risk assessments, system generated reports, third-party assessments that were performed to identify control weaknesses, strategy, risks, and any anomalies that have occurred that represent a security risk. Tickets are opened if actionable items are identified.

The annual company-wide risk assessment identifies and assesses the following areas that could affect Sangoma's system of internal controls:

A. Assets and environment;
B. Business objectives and operations;
C. Financial strategies;
D. Vendors, business partners and direct and contract employees;
E. Regulatory changes;
F. Changes in the threat landscape;
G. Information technology;
H. Fraud risk; and,
I. Determining a risk mitigation strategy.

Sangoma's Security Incident Response Plan includes steps for timely identification, severity classification, investigation, reporting, and resolution of incidents, as well as communication to the affected parties. Identified or reported incidents are communicated to the appropriate teams and are tracked and logged through remediation in the ticketing system. The remediation results are communicated to Security and Legal Teams. Sangoma's website has a support page that provides users with documentation regarding security and availability best practices to be implemented by customers. Sangoma's Security Team tests its Security Incident Response Plan annually. Changes to the policy and lessons learned are documented and are communicated to the Executive Risk Committee.

Security incidents are assigned a severity classification by the Security Team using the Incident Security Classification section in the Security Incident Response Plan which includes details on how to classify potential incidents as low, medium, or high. A minimum of 60 days of backups are encrypted and stored and are available for restoration to assist in response to recovery from a security incident. Database backups are tested by the appropriate team.

Sangoma's Security Incident Response Plan requires a "lessons learned" session after every major security incident, that documentation of the incident is maintained within an incident response ticket, and a Follow Up Report is created for all major security incidents. The change management policy or playbooks are updated to mitigate exploited vulnerabilities to prevent similar incidents in the future.

Change Management

The Cybersecurity Policy, addressing the system development life cycle, includes the design, acquisition, implementation, configuration, testing, modification, and maintenance of systems infrastructure and software. This policy specifies the processes for documenting and authorizing changes to systems infrastructure. Changes to the system's infrastructure and software configurations are reviewed and approved during the Weekly Security Team meeting and change tickets are developed to implement the changes. These changes require documentation of test plans, backout procedures, and approval for normal and emergency changes which are used to implement the changes in the environment. These changes are also limited to authorized users on the appropriate team.

Internal and external environments are scanned continually by the Security Team to identify security vulnerabilities. High and Critical vulnerabilities are reviewed during the weekly Security Team meeting and internal tickets or change controls are entered into the system for remediation in accordance with the Risk Management Policies. Application and infrastructure changes to operating systems and software are authorized, tested and approved to follow the Change Management Process which requires Security Team approval for normal and emergency changes prior to implementation.

The Security Team meets monthly to review vulnerability scans, risk assessments, system generated reports, third-party assessments that were performed to identify control weaknesses, strategy, risks, and any anomalies that have occurred that represent a security risk. Tickets are opened if actionable items are identified.

A third-party performs a penetration test against the Sangoma application platform for software vulnerabilities after every version release. Test results rated as medium or above are reported to the Executive Risk Committee, have developed and documented mitigation strategies, are tracked in the internal ticketing system, and are reviewed during the monthly Security Team meeting until they are resolved.

Availability Controls

Sangoma IT Management, Information Security, System Engineering, and Network Engineering personnel all support Disaster Recovery, Contingency, and Incident Response plans for Sangoma. This is to ensure that if any portion of a plan is implemented, Sangoma staff are aware that portions of other plans may also need to be enacted depending on the particular scenario. The Sangoma Recovery Planning, Incident Reporting Policy, and Incident Response Policies are available on the Company's internally shared site and are available to appropriate users. Sangoma's COO or CIO and CISO review and approve the Recovery Planning and Incident Response Policies, and are also aware of interrelation between these plans, and ensure that the plans reference and complement each other.

Backups are mirrored throughout third-party data centers in which Sangoma operates, and the appropriate Department is notified in the event of failures. The ability to add, modify, and delete backup schedules is limited to the appropriate Department. The Sangoma Recovery Planning and Incident Response Policies, are available on the Company's internally shared site and are available to appropriate users. The ability to add, modify and delete backup schedules is limited to the appropriate department. A documented Business Continuity Plan and Business Impact Analysis are in place in the event of a failure, and the plan is tested annually.

Management obtains and reviews SOC reports from its subservice organizations for adequacy of its physical security and environmental protections.

Redundant infrastructure is in place at the boundary of the System to meet its availability commitments. These systems are in active/active or active/passive states per the manufacturer recommendations and allow for maintenance or failures to cause little or no impact to redundant services. Sangoma monitors the production infrastructure on a 7x24x365 basis, and investigates discrepancies identified that may affect the System's availability.

Sangoma’s users are provided with toll free numbers to report security and availability issues that are then internally routed to the appropriate team for action. Sangoma’s users can alternatively email the support team to have a ticket opened for them.

Control Activities

Control activities are the policies and procedures that help address risk and ensure management directives are carried out. Control activities, whether automated or manual, related to the achievement of specific criteria and are applied at various levels throughout the organization.

Formal written policies for significant functions and processes have been developed and communicated throughout the organization. Policies are updated annually by an assigned policy owner and are reviewed and approved by designated members of management. Policies contain requirements around the Security and Availability of Client data and include (but not limited to) topics such as:

- Account administration
- Data classification, retention and destruction
- Security incident reporting and response
- Security awareness training and education
- Change management and application development

Sangoma performs an annual risk assessment to identify potential fraud threats that could impair system security, analyzes the significance of risks associated with the identified threats, determines mitigation strategies for those risks. Identified risks are rated using a risk evaluation process and ratings reports are reviewed by the Security Team.

Control recommendations made by the Security Team to remedy risks identified during the annual company-wide risk assessment, which are documented in the risk assessment, are reviewed and actioned (approved, denied, modified) by the Executive Risk Committee.

The Security Team meets monthly to review vulnerability scans, risk assessments, system generated reports, third-party assessments that were performed to identify control weaknesses, and strategy, risks, and any anomalies that have occurred that represent a security risk. Tickets are opened if actionable items are identified.

Sangoma utilizes its policies and procedures to implement control activities. Sangoma policies define the frequency of the control and the process owners to complete the control activities within a specified time frame and take any necessary corrective actions.

Sangoma has implemented its Information Security Policies that are reviewed and approved annually by the CISO or the CTO, over significant aspects of operations, which include:

a. security requirements for authorized users;
b. data classification and associated protection, access rights, retention and destruction requirements;
c. risk assessment;
d. access protection requirements;
e. user provisioning and deprovisioning;
f. responsibility and accountability for security;
g. responsibility and accountability for system changes and maintenance;
h. change management;
i. security and other incidents identification, response and mitigation;
j. security training; and,
k. information sharing and disclosure.

An Executive Risk Committee has been implemented and requires the committee to meet quarterly, record meeting minutes, be comprised of at least one member having security experience, and reports to the CEO/BoD on a quarterly basis. The Security Team reviews security assessments and/or control attestation reports for in-scope vendors and subservice organizations during onboarding and annually thereafter to monitor for deficiencies that may introduce risk to Sangoma. Any findings and/or recommendations from the Security Team are documented and reviewed by the Security Steering Committee who will make recommendations to the Executive Risk Committee on how the risks will be mitigated. Job descriptions, outlining authority, roles and responsibility, are reviewed, approved, and maintained by People and Talent and are reviewed, updated, and approved by the hiring managers as needed. Job descriptions are reviewed by the employee and manager annually as part of the employees' performance evaluation. Sangoma's information security policies are reviewed and updated by the Security Team to include control activities to mitigate risks identified in the risk assessment and are approved by CISO and CTO annually.

Complementary User-Entity Controls

The policies and procedures that Sangoma has put in place to govern its service delivery to customers does not remove the responsibility of users to implement their own complementary internal control structure. User entities should evaluate their internal controls in conjunction with the controls put in place by Sangoma on a regular basis and update their controls appropriately to reflect any changes in their operating environment.

In designing its system, Sangoma contemplated that certain complementary controls would be implemented by user entities to achieve certain criteria applicable to security and availability. The complementary user entity controls are included within the description below and Section 3 of this report.

User Entity Control	Associated Criteria Group
Customers are required to send Sangoma information in a secure format that is defined in the Master Services Agreement.	Common Criteria Group 6
Customers are required to notify Sangoma of any changes in user accounts that can access the SFTP site.	Common Criteria Group 6

Complementary Subservice Organization Controls

The subservice organizations are responsible for the physical access to the infrastructure components supporting the services which are provided by Sangoma. The Description indicates that certain applicable trust services criteria can only be met if the subservice organization controls, assumed in the design of Sangoma's controls, are suitably designed and operating effectively along with related controls at the service organization. The following list presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at the subservice organization:

Complementary Subservice Organization Controls	Associated Criteria Group
CoreSite – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Chicago, IL; Reston, VA; Los Angeles, CA; Atlanta, GA; Denver, CO	Common Criteria Group 6
Equinix – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Chicago, IL; Sydney, Australia; Toronto, Canada	Common Criteria Group 6
Digital Realty – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Atlanta, GA; New York, NY; Clifton, NJ; Dallas, TX; San Francisco, CA; Marseille, France	Common Criteria Group 6
Lunavi – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Seattle, WA	Common Criteria Group 6
Crown Castle – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Los Angeles, CA	Common Criteria Group 6
Databank – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Dallas, TX	Common Criteria Group 6
Switch – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Las Vegas, NV	Common Criteria Group 6

Complementary Subservice Organization Controls (continued)	Associated Criteria Group
365 Datacenters – should establish controls to restrict access to the following Data Centers for the physical and location infrastructure: Reston, VA	Common Criteria Group 6
Amazon AWS – should establish controls to restrict access to the following resources for virtual and location infrastructure: Cloud Compute, Cloud Storage	Common Criteria Group 6

Sangoma US, Inc.'s Trust Services Criteria and Related Controls

Mapping of Control Activities to Criteria for Security and Availability

Criteria Reference #	Trust Services Criteria Description	Control #
Common Criteria Related to Organization and Management		
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	1, 2, 3, 5, 6, 9, 12
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1, 4, 40
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	5, 11
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	9, 10, 12, 14, 15, 16
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	7, 8, 13, 14, 17, 92
Common Criteria Related to Communication and Information		
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	85, 86
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	10, 11, 17, 18, 19, 66

Criteria Reference #	Trust Services Criteria Description	Control #
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	18, 20, 21, 22, 23, 55, 67, 93, 109
Common Criteria Related to Risk Management and Design and Implementation of Controls		
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	24, 26, 28, 34, 61, 94
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	26, 30, 34
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	25, 26, 38
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	34
Common Criteria Related to Monitoring		
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	29, 31, 37, 87, 88, 89, 90, 95
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	17, 32, 37, 95

Criteria Reference #	Trust Services Criteria Description	Control #
Common Criteria Related to Control Activities		
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	25, 27
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	27, 33, 35
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	11, 33, 36, 39, 40, 95
Common Criteria Related to Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	37, 41, 42, 43, 44, 46, 47, 49, 50, 52, 54, 71, 74, 75
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	44, 68, 69
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	44, 47, 68

Criteria Reference #	Trust Services Criteria Description	Control #
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, datacenter facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	48
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	45, 73
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	54, 72
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	52, 53, 54, 74, 75, 99
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	29, 37, 51, 70, 76, 98
Common Criteria Related to System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	29, 37, 82, 83
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	33, 34, 37

Criteria Reference #	Trust Services Criteria Description	Control #
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	18, 55, 58, 60
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	18, 56, 61, 62
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	18, 57, 58, 77
Common Criteria Related to Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	33, 59, 63, 64, 78, 79, 80, 81
Common Criteria Related to Risk Management		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	58, 91
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	84, 96, 97

Criteria Reference #	Trust Services Criteria Description	Control #
Common Criteria Related to Availability		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	100, 101, 102, 106, 107, 108, 109
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	103, 105
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	77, 104, 105, 107

Testing Procedures Performed by Independent Service Auditors

In addition to the tests listed below for each control specified by Sangoma, ascertained through inquiry with management and the control owner that each control activity listed below operated as described.

Note: Although not sequential, the below mapping demonstrates that the trust services criteria have been mapped completely and accurately to Sangoma controls.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
1.	CC1.1, CC1.2	A Board of Directors has been implemented and operates under a Charter that outlines the responsibility to oversee the development and performance of the Company and which each member is required to acknowledge their understanding of their responsibility and review and approve at least annually.
2.	CC1.1	The Board of Directors operates under a charter that includes discussion of a business code of conduct that establishes ethical and integrity values which members are required to sign off acknowledging their understanding upon joining the board.
3.	CC1.1	The Board of Directors reviews and approves the Charter on an annual basis.
4.	CC1.2	The Board of Directors' Charter establishes the number of members, their qualifications, oversight responsibilities, at least two of its members be independent of management, required meeting frequencies, and background and skills of each member be reviewed upon invitation to join.
5.	CC1.1, CC1.3	Sangoma has an established organizational chart for the Company and job descriptions that include key considerations of authority and responsibility, as well as appropriate lines of reporting for key employees. The organizational chart is reviewed and approved by a the CHRO at least annually.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
6.	CC1.1	Sangoma has implemented a Code of Business Conduct and Ethics which is reviewed and approved by the Board of Directors annually.
7.	CC1.5	Sangoma provides internal and external personnel with means to report ethics concerns and questions as noted within the Whistleblower Policy.
8.	CC1.5	The Board of Directors sets goals for performance and evaluation criteria including incentives, other rewards, and sanctions for the entire organization and reviews and approves those goals annually.
9.	CC1.1, CC1.4	Internal users of the system are required to sign a Code of Conduct upon hire and annually thereafter that establishes integrity and ethical values and the consequences for violations.
10.	CC1.4, CC2.2	Internal users undergo annual security training and are required to confirm their understanding of and compliance with the security policies and the Acceptable Use Policy upon hire and annually thereafter.
11.	CC1.3, CC2.2, CC5.3	Job descriptions, outlining authority, roles and responsibility, are reviewed, approved, and maintained by People and Talent and are reviewed, updated, and approved by the hiring managers as needed. Job descriptions are reviewed by the employee and manager annually as part of the employees' performance evaluation.
12.	CC1.1, CC1.4	As part of the new hire and offer letter acceptance process, personnel agree to be verified against regulatory screening databases, including criminal checks and are reviewed by People and Talent. Based on the candidates' role, technical users of the system undergo a technical assessment as part of their onboarding and skill verification process.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
13.	CC1.5	The Acceptable Use Policy outlines security standards for the use of electronic devices and network resources and sanctions for violations thereof which internal users are required to sign off on upon hire and annually thereafter.
14.	CC1.4, CC1.5	People and Talent and the employees' manager review employees' performance annually to develop and align employees' goals with Sangoma's objectives. The employees and their managers both sign the performance review.
15.	CC1.4	Violations of the Code of Conduct are investigated timely and may result in disciplinary actions up to and including probation, suspension and termination of employment. Report of significant cases will be summarized and presented to the CEO and CFO as needed.
16.	CC1.4	People and Talent maintains a list of contractors that is reviewed on a quarterly basis to verify adherence of Sangoma's corporate governance documents and identify any contracts that have been completed.
17.	CC1.5, CC2.2, CC4.2	The Security Team reports on identified deficiencies within internal controls, suggested remediations, and the appropriate control owner to the Operational Team Lead on a monthly basis that includes summaries of any completed third-party assessments of internal controls and automated vulnerability scans.
18.	CC2.2, CC2.3, CC7.3, CC7.4, CC7.5	Sangoma's Security Incident Response Plan include steps for timely identification, severity classification, investigation, reporting, and resolution of incidents, as well as communication to the affected parties. Identified or reported incidents are communicated to the appropriate teams and are tracked and logged through remediation in the ticketing system. The remediation results are communicated to Security and Legal Teams.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
19.	CC2.2	Sangoma supports its Security Policies by designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system that is reviewed and approved by the Security Team on an annual basis and is available to all system users on the Company's cloud share. Only the Infrastructure, Security, Legal, and Compliance Teams have access to make updates to these documents.
20.	CC2.3	Sangoma's users are alerted in the event of a security or maintenance-related issue via email and/or through its Trust Site.
21.	CC2.3	Sangoma communicates its security commitments to external users, with whom it shares information, through formal agreements.
22.	CC2.3	The Security Team reviews the Description of Services as it relates to security on an annual basis. This Description of Services is communicated to appropriate business partners and clients via agreed upon means.
23.	CC2.3	Sangoma maintains a list of complementary end user controls that are provided to the clients through its Terms of Service, which is included in its Subscription Agreement and is available on Sangoma's external website.
24.	CC3.1	The Security Team presents the annual company-wide risk assessment and management's mitigation strategies to the Executive Risk Committee. Business unit owners follow their standard processes for remediation, tracking, and approvals as needed.
25.	CC3.3, CC5.1	Sangoma performs an annual risk assessment to identify potential fraud threats that could impair system security, analyzes the significance of risks associated with the identified threats, and determines mitigation strategies for those risks. Identified risks are rated using a risk evaluation process and a ratings report is reviewed by the Security Team.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
26.	CC3.1, CC3.2, CC3.3	All discovered risks that could impact security are entered into the risk register and assigned an owner depending on the risk type, tracked until resolved and approved by the Security Team documenting the risk has been mitigated.
27.	CC5.1, CC5.2	Control recommendations made by the Security Team to remedy risks identified during the annual company-wide risk assessment, which are documented in the risk assessment, are reviewed and actioned (approved, denied, modified) by the Executive Risk Committee.
28.	CC3.1	During the annual company-wide risk assessment, risks are identified as very low, low, moderate, high, or very high based on the likelihood of occurrence and measured based on the risk measurement criteria approved by the Security Team to evaluate the impact on the people, company assets, locational risks, assessment risks, financial risks, third party risks, fraud risks, regulatory risks, and fundamental principles of the organization.
29.	CC4.1, CC6.8, CC7.1	Internal and external environments are scanned continually by the Security Team to identify security vulnerabilities. High and Critical vulnerabilities are reviewed during the weekly Security Team meeting and internal tickets or change controls are entered into the system for remediation in accordance with the Risk Management Policies.
30.	CC3.2	The Executive Risk Committee meets quarterly to discuss strategy and operations, financial results, risk considerations and other factors critical to the business.
31.	CC4.1	Sangoma engages with a third party to perform an external penetration test on the environment on a twice-annual basis, and the results are communicated to the Security Team. Any critical findings are remediated within 60 days.
32.	CC4.2	The Security Team monitors the corrective action plan on a monthly basis to verify deficiencies of internal controls are remediated on a timely basis.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
33.	CC5.2, CC5.3, CC7.2, CC8.1	The Security Team meets monthly to review vulnerability scans, risk assessments, system generated reports, and third-party assessments that were performed to identify control weaknesses, strategy, risks, and any anomalies that have occurred that represent a security risk. Tickets are opened if actionable items are identified.
34.	CC3.1, CC3.2, CC3.4, CC7.2	The annual company-wide risk assessment identifies and assesses the following areas that could affect Sangoma's system of internal controls: A. Assets and environment; B. Business objectives and operations; C. Financial strategies; D. Vendors, business partners and direct and contract employees; E. Regulatory changes; F. Changes in the threat landscape, G. Information technology, H. Fraud risk, and; I. Determining a risk mitigation strategy.
35.	CC5.2	Sangoma utilizes its policies and procedures to implement control activities. Sangoma policies define the frequency of the control and the process owners to complete the control activities within a specified time frame and take any necessary corrective actions.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
36.	CC5.3	Sangoma has implemented its Information Security Policies that are reviewed and approved annually by the CISO or the CTO, over significant aspects of operations, which include: a. security requirements for authorized users; b. data classification and associated protection, access rights, retention and destruction requirements; c. risk assessment; d. access protection requirements; e. user provisioning and deprovisioning; f. responsibility and accountability for security; g. responsibility and accountability for system changes and maintenance; h. change management; i. security and other incidents identification, response and mitigation; j. security training; and, k. information sharing and disclosure.
37.	CC4.1, CC4.2, CC6.1, CC6.8, CC7.1, CC7.2	Sangoma maintains a SIEM that aggregates and evaluates system logs to monitor network, database, server, and domain events to detect any unauthorized access. The logging system provides alerting based on rulesets identified by management, which is monitored by the Infrastructure and Security Teams via email when an event is triggered, and is used to: identify potential security threats, vulnerabilities, or breaches; and detect unusual system activity.
38.	CC3.3	Sangoma performs a fraud risk assessment that identifies risks by assessing pressures, opportunities, attitudes and rationalizations of finance staff and to those in a position to influence them.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
39.	CC5.3	Sangoma's information security policies are reviewed and updated by the Security Team to include control activities to mitigate risks identified in the risk assessment and are approved by the CISO and CTO annually.
40.	CC1.2, CC5.3	An Executive Risk Committee has been implemented and requires the committee to meet quarterly, record meeting minutes, be comprised of at least one member having security experience, and reports to the CEO/BoD on a quarterly basis.
41.	CC6.1	Network accounts will be locked out after 3-5 unsuccessful login attempts depending on system requirements.
42.	CC6.1	Network and application administration user accounts have been restricted to appropriate teams.
43.	CC6.1	Predefined user groups are utilized to assign role-based access privileges to restrict authorized users' access.
44.	CC6.1, CC6.2, CC6.3	Requests for additional access above the user's role to the system are made by the user and approved by the manager. Access requests are documented and tracked in Sangoma's internal ticketing system.
45.	CC6.5	The Asset Management Policy requires all assets capable of storing customer data have the data destroyed/sanitized to erase all data once the asset is identified as no longer required to meet the Company's objectives.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
46.	CC6.1	The Access Control Policy requires minimum password complexity to be configured when accessing internal Sangoma systems. The Access Control Policy requires network accounts will be configured to be locked out after a limited number of unsuccessful login attempts and have the following minimum configuration: - At least eight characters, and; - Passwords must also contain 3 of the 4 of the following requirements: - Contain at least 8 alphanumeric characters; - Contain both upper and lower case letters; - Contain at least one number, and; - Contain at least one special character (e.g.: !@#$%^) in certain environments.
47.	CC6.1, CC6.3	The Security Team performs quarterly reviews of the privileged user groups of the corporate network, and applications to verify that access is appropriate based on role to verify the role has the least required access for the job function.
48.	CC6.4	Sangoma employs locks, or other access control methods to physically secure its office location to restrict access to authorized personnel only.
49.	CC6.1	Sangoma provides users with guidelines to keep their passwords secure which is documented in the Acceptable Use Policy.
50.	CC6.1	Sangoma requires multi factor authentication (“MFA”) to gain access to production application servers in the environment.
51.	CC6.8	Sangoma scans all incoming and outgoing corporate emails for malicious software which is quarantined, and a notification is sent out based on incoming or outgoing destinations, if found.
52.	CC6.1, CC6.7	Sangoma utilizes AES-256 encryption on all data stored at rest and in data backups. Backup access is limited to appropriate users.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
53.	CC6.7	When email is sent from the system, the content of the messages and attachments is scanned to identify potential private data. The e-mail is encrypted in transit.
54.	CC6.1, CC6.6, CC6.7	When internal or external users connect with in-scope systems; VPN, SSL/TLS, SSH, SFTP, or other transport encryption technologies are used for defined points of connectivity.
55.	CC2.3, CC7.3	Sangoma communicates security incidents to impacted parties based on the severity classification in the Security Incident Response Plan.
56.	CC7.4	The Company has implemented the Security Incident Response Plan which includes procedures for Incident Identification, Response, Classification, Communication, and Follow up Lessons Learned for security incidents to the impacted parties as they are identified or reported to the Security Team which are tracked and logged through remediation.
57.	CC7.5	Sangoma's Security Incident Response Plan requires a lessons learned session after every major security incident, documentation of the incident be maintained within an incident response ticket, and a Follow Up Report is created for all major security incidents. The change management policy or playbooks are updated to mitigate exploited vulnerabilities to prevent similar incidents in the future.
58.	CC7.3, CC7.5, CC9.1	Sangoma's Security Team tests its Security Incident Response Plan annually. Changes to the policy and lessons learned are documented and are communicated to the Executive Risk Committee.
59.	CC8.1	A third-party performs a penetration test against the Sangoma application platform for software vulnerabilities after every version release. Test results rated as medium or above are reported to the Executive Risk Committee, have developed and documented mitigation strategies, are tracked in the internal ticketing system, and are reviewed during the monthly Security Team meeting until they are resolved.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
60.	CC7.3	Sangoma's website has a support page that provides users with documentation regarding security and availability best practices to be implemented by customers.
61.	CC7.4	Security incidents are assigned a severity classification by the Security Team using the Incident Security Classification section in the Security Incident Response Plan which includes details on how to classify potential incidents as low, medium, or high.
62.	CC7.4	Security incidents are responded to by the Security Team based on the Security Incident Response Plan which includes detailed procedures, based on severity, to assess, contain, and mitigate the incident and that requires a lessons learned to be performed to prevent or address the security incident.
63.	CC8.1	The Cybersecurity Policy, addressing the system development life cycle, includes the design, acquisition, implementation, configuration, testing, modification, and maintenance of systems infrastructure and software.
64.	CC8.1	The Cybersecurity Policy specifies the processes for documenting and authorizing changes to systems infrastructure.
65.	CC3.1	The Company performs a company-wide risk assessment that includes the identification of risks that could impact the operations of the business, information technology, and fraud risks on an annual basis.
66.	CC2.2	The Security Team ensures that Sangoma's security commitments and system requirements are current by reviewing amendments or changes to client contracts and communicating changes to these requirements to the process owner of the control affected by the change.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
67.	CC2.3	Sangoma communicates user security commitments, with whom it obtains information, through the Terms of Service or similar agreement based on product listed on the Company's website and as part of the client contract.
68.	CC6.2, CC6.3	A ticket is opened that tracks and notifies the appropriate teams when access has been revoked and network access is removed within 1 business day. This ticket is tracked through completion.
69.	CC6.2	Access requests have a ticket opened and routed to the appropriate team to grant access based on role.
70.	CC6.8	Anti-virus software is deployed on all devices and is reviewed by the IT Team quarterly to ensure anti-virus software is up to date and operational.
71.	CC6.1	The IT Team enables full disk encryption when issuing laptops to users.
72.	CC6.6	Sangoma has an Intrusion Detection System ("IDS") to monitor Sangoma's network and the production environment by notifying the Security Team of potential security incidents.
73.	CC6.5	Sangoma has implemented the Asset Management Policy which includes policies and procedures on the tracking of physical assets from purchase to destruction, requiring all assets capable of storing customer data obtain a certificate of destruction upon destruction of the asset.
74.	CC6.1, CC6.7	Sangoma's firewalls are restricted to the Security Team and are configured to limit unnecessary ports, protocols, and services which are reviewed monthly by the Security Team.
75.	CC6.1, CC6.7	Sangoma's network is segmented using subnets and VDOMs/VRFs/VPCs to restrict access and movement of data between segments to support isolation in event of a security incident and is reviewed annually by the Security Team.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
76.	CC6.8	Sangoma's IT Team manages a corporate endpoint managed firewall solution on user computers and IT servers. Product teams maintain servers in the production product environments.
77.	CC7.5, A1.3	A minimum of 60 days of backups are encrypted and stored and are available for restoration to assist in response to recovery from a security incident. Database backups are tested by the appropriate team.
78.	CC8.1	Application and infrastructure changes to operating systems and software are authorized, tested, and approved to follow the Change Management Process which requires Security Team approval for normal and emergency changes prior to implementation.
79.	CC8.1	Changes to systems infrastructure and software configurations are reviewed and approved during the Weekly Security Team meeting and change tickets are developed to implement the changes.
80.	CC8.1	Infrastructure changes are limited to authorized users on the appropriate team.
81.	CC8.1	Infrastructure changes require documentation of test plan, back out procedures, and approval for normal and emergency changes which are used to implement the changes in the environment.
82.	CC7.1	The Security Team monitors the infrastructure and software using a device management system that measures compliance with company standards on an ongoing basis.
83.	CC7.1	The Security Team uses software to scan for and apply operating system and application patches on Servers and Workstations. A member of the Security Team reviews patches monthly and releases appropriate patches following the change management procedures. Exceptions are noted in the ticketing system.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
84.	CC9.2	The appropriate team ensures all access to confidential information or ability to impact the security of the system by an offboarded vendor is revoked by following the Third Party Policy.
85.	CC2.1	The Executive Risk Committee formally approves controls which are evaluated and tested on an annual basis by a separate functional department from the process or control owner.
86.	CC2.1	The CISO reports the results of the internal audit to the Security Team on an annual basis, who reviews and approves the action plan prepared by management.
87.	CC4.1	An internal audit, including an assessment of Sangoma's information security, is performed annually by the Security Team. Results from the internal audit are reported to management and the Executive Risk Committee.
88.	CC4.1	On a quarterly basis, an assessment is performed on the audit plan and scope of the audit to identify potential changes impacting Sangoma's risk profile and is presented to the Security Steering Committee.
89.	CC4.1	Sangoma has developed an internal audit process which requires a different member other than the process owner to validate internal controls on an annual basis. Results are documented, communicated, and tracked.
90.	CC4.1	Sangoma's internal audit program identifies process owners from all levels of management and includes a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment process.
91.	CC9.1	As part of companywide risk assessment process, Sangoma has an insurance policy in place to minimize the financial impact of a cyber loss event.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
92.	CC1.5	Upon onboarding of a High Risk vendor and annually thereafter, the Security Committee reviews the formal service agreements and/or Terms of Service with High Risk vendors to outline and document the security requirements that will be followed by each party. These commitments and each party's adherence to them will be reported to the Executive Risk Committee.
93.	CC2.3	Formal information sharing agreements are in place with High Risk vendors. These agreements include security commitments applicable to that vendor.
94.	CC3.1	The Legal and Security Committee reviews client contracts that have material changes (amendments or changes) upon execution of the contract or when renewed for service commitments and system requirements and incorporates them into the annual risk assessment to identify risks that could impact them and develop mitigation strategies.
95.	CC4.1, CC4.2, CC5.3	The Security Team reviews security assessments and/or control attestation reports for in-scope vendors and subservice organizations during onboarding and annually thereafter to monitor for deficiencies that may introduce risk to Sangoma. Any findings and/or recommendations from the Security Team are documented and reviewed by the Security Steering Committee who will make recommendations to the Executive Risk Committee on how the risks will be mitigated.
96.	CC9.2	Sangoma's High Risk vendor approval process requires the vendor agreements to include security policies, procedures, and related controls that are required to be in place.
97.	CC9.2	Vendor risk assessments are performed by the Security Committee before engagement and annually for High Risk vendors and subservice organizations with access to confidential data or the ability to affect the security of the system.
98.	CC6.8	Baseline server configurations are reviewed and updated annually, or as needed, by the appropriate Team.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
99.	CC6.7	Data backups of critical elements are performed nightly and replicated to another data center. Real-time replication of journal files is configured for the collections system.
100.	A1.1	Sangoma IT Management, Information Security, System Engineering, and Network Engineering personnel all support Disaster Recovery, Contingency, and Incident Response plans for Sangoma. This is to ensure that if any portion of a plan is implemented, Sangoma staff are aware that portions of other plans may also need to be enacted depending on the particular scenario.
101.	A1.1	Sangoma's COO or CTO and CISO review and approve the Recovery Planning and Incident Response Policies, and are also aware of interrelation between these plans, and ensure that the plans reference and complement each other.
102.	A1.1	Backups are mirrored throughout third-party data centers in which Sangoma operates, and the appropriate Department is notified in the event of failures.
103.	A1.2	The ability to add, modify and delete backup schedules is limited to the appropriate Department.
104.	A1.3	The Sangoma Recovery Planning and Incident Response Policies are available on the Company's internally shared site and are available to appropriate users.
105.	A1.2, A1.3	A documented Business Continuity Plan and Business Impact Analysis is in place in the event of a failure, and the plan is tested annually.
106.	A1.1	Management obtains and reviews SOC reports from its subservice organizations for adequacy of its physical security and environmental protections.

Control #	Criteria Reference #	Sangoma US, Inc. Control Description
107.	A1.1, A1.3	Redundant infrastructure is in place at the boundary of the System to meet its availability commitments.
108.	A1.1	Sangoma monitors the production infrastructure on a 7x24x365 basis, and investigates discrepancies identified that may affect the System's availability.
109.	CC2.3, A1.1	Sangoma's users are provided with a toll free number to report security and availability issues that are then internally routed to the appropriate team for action.