Auvik Platform

Service Organization Control Report

(SOC 2+ ISO 27001 Type I)

Report on Suitability of the Design of Controls to Meet the Criteria for the Security Trust Services Criteria plus ISO 27001 Control Descriptions

As at September 28, 2018

Table of Contents

Phone 416-865-0111
Fax 416-367-3912
www.bdo.ca

BDO Canada LLP - National
20 Wellington Street East,
Suite 500
Toronto, ON M5E 1C5

Section I: Independent Service Auditor's Report

To: Management of Auvik Networks Inc.

Scope

We have examined the Auvik Networks Inc. ("Auvik") description of its cloud based network management system (Auvik Platform) in "Section III: Management's Description of the Auvik Platform ("description") as at September 28, 2018 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 Auvik Platform that may be useful when assessing the risks arising from interactions with Auvik's system, particularly information about system controls that Auvik has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to (applicable trust services criteria) set forth in TSC section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria), and the compliance objectives set forth in ISO/IEC 27001:2013 Information Security Management Systems Requirements (ISO 27001 criteria).

Auvik uses three service organizations to aid their platform for network management: Amazon Web Services to provide cloud hosting for their production environment; Salesforce to store customer contact information, subscription status, and other related information; Auvik also uses the services of Zuora to process e-subscription billing for Auvik's customers. The description does not disclose the controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Auvik, to achieve Auvik's service commitments and system requirements based on the applicable trust services criteria and ISO 27001 criteria. The description presents Auvik's controls, the applicable trust services criteria and ISO 27001 criteria, and the complementary user entity controls assumed in the design of Auvik's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such control.

Service Organization's Responsibilities

Auvik is responsible for its service commitments and system requirements and for designing, implementing controls within the system to provide reasonable assurance that Auvik's service commitments and system requirements were achieved. Auvik has provided the accompanying assertion titled "Section II Management's Assertion" (assertion) about the description and the suitability of design of controls stated therein. Auvik is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and ISO 27001 criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

The information included in Section V "Mapping Trust Services Criteria to ISO 27001 Control Descriptions," is presented by Auvik to provide additional information and is not a part of the description. Information on the mapping of Auvik's Trust Services Criteria and related controls to ISO 27001 has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls to achieve Auvik's service commitments and system requirements based on the applicable trust services criteria.

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 and ISO 27001 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 and ISO 27001 criteria
- Testing the design of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and ISO 27001 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 users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

The projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of controls to meet the applicable trust services criteria and ISO 27001 criteria is subject to the risks that controls may become inadequate because for changes in in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matters

We did not perform any procedures regarding the operating effectiveness of the 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 the Auvik Platform that was designed and implemented as at September 28, 2018, in accordance with the description criteria;

(b) the controls stated in the description were suitably designed as at September 28, 2018 to provide reasonable assurance that Auvik's service commitments and system requirements would be achieved based on the applicable trust services criteria and ISO 27001 criteria, if its controls operated effectively as of that date and if the user entities applied the complementary controls assumed in the design of Auvik's controls throughout that period.

Restricted Use

This report is intended solely for the information and use of Auvik; user entities of the Auvik Platform as at September 28, 2018 and prospective user entities, practitioners providing services to such 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 organization's system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity 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 and ISO 27001 criteria
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria 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.

BDO Canada LLP

Chartered Professional Accountants
November 5, 2018
Toronto, ON

Section II: Management's Assertion

We have prepared the accompanying description of the cloud based network management system (Auvik Platform) in "Section III: Management's Description of the Auvik Platform" ("description") as at September 28, 2018 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 Auvik Platform that may be useful when assessing the risks from interactions with Auvik's system, particularly information about system controls that Auvik has designed, implemented, and operated to provide reasonable assurance that its service commitments and systems requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSC section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria), and the compliance objectives set forth in ISO/IEC 27001:2013 Information Security Management Systems Requirements (ISO 27001 criteria).

Auvik uses three service organizations to aid their platform for network management: Amazon Web Services to provide cloud hosting for their production environment; Salesforce to store customer contact information, subscription status, and other related information; Auvik also uses the services of Zuora to process e-subscription billing for Auvik's customers. The description does not disclose the controls at the subservice organizations.

The description also indicates that user entity controls that are suitably designed, along with the controls at Auvik, to achieve Auvik's service requirements and systems requirements based on the applicable trust services criteria and ISO 27001 criteria. The description presents Auvik's controls, the applicable trust services criteria, and ISO 27001 criteria and the complementary user entity controls assumed in the design of Auvik's controls.

We confirm, to the best of our knowledge and belief, that:

(a) the description presents Auvik's Platform as at September 28, 2018, in accordance with the description criteria.
(b) the controls stated in description were suitably designed and implemented as at September 28, 2018, to provide reasonable assurance that Auvik's service commitments and system requirements would be achieved based on the applicable trust services criteria and ISO 27001 criteria and if the user entity applied the complementary controls assumed in the design of Auvik's controls operated effectively.

Kevin Vye
Associate Vice President, IT & Security
November 5, 2018

Section III: Management's Description of Auvik's Platform

Overview of the Auvik Platform

Auvik is a cloud-based system that provides unprecedented insight into networks and automates complex and time-consuming tasks. Auvik keeps network maps and documentation up to date in real-time, captures and manages device configurations, monitors network performance, alerts you to potential network issues, and more. Data security was built into Auvik from the beginning. We've followed industry best practices to ensure Auvik is as safe and secure as the most well-known and respected cloud-based offerings

Scope of Report

This document provides the reader with an overview of the pertinent services, policies and procedures that are in place. This report is intended to describe only the controls of the Auvik Platform.

System Description

Auvik is responsible for operating the environment in which the Auvik Platform resides. This environment runs inside a data center and is made of both logical and physical components which, when properly deployed, provide a secure and robust service for Auvik's customers. These components include:

- The physical data center, including the environment and security controls are hosted in the Public Cloud. In Public Cloud data centers, the hardware infrastructure is managed completely by the Public Cloud vendor.
- Networking equipment, including WAFs, routers, firewalls, load balancers, VPNs and switches.
- Server, appliances and storage. This includes web, application and database servers, storage appliances, and utilities such as mail servers, Active Directory servers, and monitoring systems.
- Operating systems, utilities and application code.

Within the demarcation point, or the point where the telecom connection ends and the Auvik network begins, Auvik is responsible for the security, availability and performance of the application. Outside the demarcation point, between the client and the Auvik environment, are networks that consist of the Public Internet, development networks, and other home and commercial networks. The environment inside the demarcation point is managed by Auvik, and is thereby subject to the controls outlined in this report.

Description of Services Provided

Services	Description
MSP administration	Multi-client account - Manage an unlimited number of clients from the parent account.
	Two-factor authentication - Apply heightened security at the global or client level.
	Roll-up dashboard - See all clients' from a single screen.
	User management - Easily control who has access to which client networks.
	PSA integrations - Integrate with key workflow tools already used for optimum efficiency.
Network topology	Automated mapping - In minutes, see a complete map of physical and logical topologies.
	Map search & filter - Quickly find and visually isolate any part of a network.

	Automated inventory - Have a profile for every device on a network at the fingertips.
	Map export - Print any map view to PDF or SVG for easy sharing or storage.
	Network documentation - Instantly know how everything on a network is connected.
	Password management - Never again forget device credentials or leave them vulnerable. Manage them securely within Auvik.
	IP address management - Get an automatic list of all the IP addresses currently in use and which devices are using them.
Network monitoring	Alerts & notifications - Stay on top of important network events with both preconfigured and customizable alerting.
	Rich statistics - Understand and improve the stability of a network with usage and health stats.
	Service monitoring - Inventory and monitor the services running on nearly any device on a network.
	Live & historic data - View network performance as it happens with 60-second polling, or dive into detailed logs.
	Context-aware data - Get relevant and actionable information tailored to each device type.
Remote management	In-app terminal - Securely access any Telnet or SSH-enabled device on a network—from anywhere.
	Remote browser - Log into any device's web interface directly from the Auvik dashboard.

People

Organizational Structure and Assignment of Authority and Responsibility

Auvik has developed an organizational structure that adequately suits the nature and scope of its business operations. The Company has developed organizational charts that internally convey employee reporting relationships, operational responsibilities, and the overall organizational hierarchy.

Board of Directors

The Board of Directors is responsible for the stewardship of the business and affairs of the Company. As such, the Board of Directors has responsibility to oversee the conduct of the Company's business, provide direction to management, and ensure that all major issues affecting the business and affairs of the Company are given proper consideration.

Human Resource Policies and Practices

Auvik's human resource department has policies and established practices that govern the hiring, termination, evaluation, promotion, and compensation of current and prospective company employees. A documented set of human resource, operational, and financial policies and procedures, along with a complete list of internal controls are made available to applicable employees via the company Wiki. Detailed job descriptions and organizational charts convey the requirements for each position. Auvik also facilitates employee development through semi-annual evaluations and training. New hire policies include the requirement that background checks be performed on all new employees prior to commencing employment with Auvik. For terminated employees, Auvik has a

formal onboarding and off boarding process to ensure timely commissioning and decommissioning of access to company records and systems.

Security Staff

Auvik has a dedicated Information Security team. This team is accountable for ensuring the security of Auvik physical and logical assets. Responsibilities of the Information Security team include but are not limited to the following:

- Monitoring of Auvik's network infrastructure and assets
- Data loss prevention
- Internal investigations and forensics
- Security policies, process and procedure compliance

Information Security staff hold various professional industry recognized designations.

Integrity and Ethical Values

Auvik Networks Inc. has programs and policies designed to promote ethical values and integrity in its various environments. All personnel are governed by several personnel policies and agreements, including a confidentiality agreement.

Information Security

Policies and Procedures

Auvik has the following security procedures and policies in place, which are owned by the AVP of IT and Security

- Policies
    - Information Security Management System Policy
    - Acceptable Use Policy
    - Access Control Policy
    - Information Classification and Handling Policy
    - Physical Security Policy
    - Remote and Mobile Computing Policy
    - Security and Privacy Incident Management Policy
    - Operational Controls Policy
    - Media Sanitization and Disposal Policy
    - Third Party Security Policy
    - Personnel Security Policy
    - Cryptography Security Policy
    - Information Security Compliance Policy
    - Code of Business Conduct and Ethics Policy
    - Internal Employee Privacy Policy
- Procedures
    - Document Control Process
    - Security and Privacy Incident Management Process
    - Risk Assessment Process
    - Internal Audit Process
    - Vulnerability Scan and Pen Test Process
    - Access Audit Process
    - Media and Sanitization and Disposal Process
    - Change Management Process
    - Release Management Process

Policies are reviewed at least annually and may be reviewed more frequently if necessary. Members of the Information Security team are authorized to perform reviews of policies with final approval for changes from the AVP of IT and Security in conjunction with the executive team. Approvals are documented in the documents revision history. Any changes to the policies or procedures are then communicated to employees via Slack and e-mail and are posted in the Wiki and accessible to all employees.

To mitigate any potential for loss or exploitation of sensitive data, Auvik maintains an Information Classification and Handling policy to determine whether the appropriate controls are in place for data of higher sensitivity. This policy classifies data into categories and specifies protection accordingly. Policy points are in place to specify privacy treatment of data. The Information Security team conducts vulnerability assessments of relevant data to ensure compliance with policy points.

Security and Privacy Awareness & Training

Auvik has a security and privacy awareness program that serves to ensure employees understand the importance of security, privacy and its intersection with their workday. New employees are required to take security and privacy training and training completion is audited throughout the year. The Information Security team leverages several security threat intelligence sources to keep up to speed on the latest and emerging security threats. This information is disseminated through regular security awareness campaigns to help ensure that Auvik staff are tested and aware of these threats and what to do in the event that they encounter them.

Control Activities and Operations

Access Control

Auvik's Access Control Policy strictly limits access to client data to only those Auvik personnel whose role requires access for support purposes and follows the least privilege principle. Auvik uses multi factor authentication (MFA) to ensure that only approved resources are accessing corporate and production systems. Access to Auvik's internal corporate network is granted by certificate based authentication with Security Assertion Markup Language (SAML) including MFA for enterprise applications and production environments. Access to the Wi-Fi network is via WPA2 authentication which utilizes AES encryption. All access is logged and auditable. Access to production and corporate systems is reviewed regularly. Should staff members change departments or leave the organization, access to the environment is changed as required or revoked.

Monitoring

In order to maintain the security, availability and performance of our customer sites, Auvik closely monitors the production environment with several monitoring tools. Proactive monitoring is conducted continuously by support and operations team. All aspects of the system are monitored including infrastructure, the network, as well as the application itself. A significant investment has been made into enterprise monitoring systems such as Application Performance Management (APM), which can see the application as it functions down to the code level and can assist in identifying potential problems before SLA impacting downtime is experienced by our customers. System events are integrated in to an enterprise grade event monitoring tool. The event monitoring tool collects and aggregates millions of events daily from the production environment and stores them centrally for event correlation, security alerting and analysis. Key alerts are presented to the Information Security team who work hand in hand with the operations team on investigating potential threats.

Data Integrity

- Data at rest
    - All sensitive customer data is encrypted at rest.
    - All data backups are stored on encrypted media.
    - All employee devices have hard drive encryption enabled.

- Data in transit
    - Data in transit is encrypted using TLS security encryption protocols with RSA encryption.

Data Used and Supported by the System

- Client Data
    - Auvik does not manage customer data. Auvik acts as the custodian of the data and works to ensure that the data is properly segregated, has the appropriate access controls applied, and is securely stored and transmitted to ensure the data remains private and secure.
- Collector Data
    - The collector is a piece of code that uses a number of protocols to gather information about the network, such as topology details, configurations, and network statistics. The collector summarizes and sends that information to the Auvik Platform over an encrypted connection.
- Application Data
    - This consists of application files and binaries, and logs data generated from applications running in the production environment.
- System Data
    - This is non-user related data generated from supporting systems in the production environment, such as system logs, monitoring data etc.
- Business Intelligence
    - Anonymized non-personal data gathered from application user interactions, connection speeds between devices, the number of bytes sent, and usage statistics for the sole purpose of analyzing, optimizing and improving the Auvik Platform.

Vulnerability Management and Patching

Auvik tests all code, third party libraries and Docker containers for security vulnerabilities before release, and regularly scans its network and systems for vulnerabilities after release. Patches go through a QA process prior to being scheduled for implementation during the next available release period.

Annual Third-Party Assessments

Auvik utilizes a third party security assessment firm to conduct penetration and web application dynamic vulnerability scans against the Auvik Platform, Auvik corporate website and Auvik offices.

Application Security

Developer Training

The application is developed using the OWASP Top Ten framework, SANS Top 25 and various security components are integrated into the build and application architecture. Security analysts regularly look for vulnerabilities through code reviews, application scans, and internally-run penetration tests. Third parties validate the technical controls by conducting annually scheduled network penetration and application vulnerability tests.

Change and Release Management

Auvik releases once every two weeks, with a scheduled deployment date of Saturday morning at 7:00 am EST. Release items are only promoted when all conditions are met and accepted by the release management committee. All changes where possible are released as code and follow the release management process. When a change cannot be committed via code it require a ticket be created, peer review and approval before the change can be made.

Definition of “Dev Done”

Stories/Bugs

- Deliverables (code, investigation, doc, test cases) review is completed (peer or SME as appropriate)
- Document any story specific configurations or environmental changes required (and made on stage)
- Deliverable has been tested against the acceptance criteria
- Bugs that violate the acceptance criteria are resolved or deferred (Project Owner decides)
- Code - Unit Tests are written and pass (80%+ coverage of story code)
- Code - No new build warnings
- Code - 100% unit test pass for the entire build (not just for the story)
- Code - Buildable and promoted to DIT (development integration test) environment
- Code - Migration scripts available if applicable
- Code - Static code scan pass
- Infrastructure – Clean vulnerability scan of third-party libraries and supporting software
- QA - Automation scripts are written and pass
- Business intent of the story has been met (Project Owner decides)

Sprints

- All tickets are complete as defined by the DoD for stories/bugs
- Sprint demo is complete, before the change is checked into develop
- Bugs verified but not fixed for stories in the sprint are logged, with rationale from Project Owner
- Code - Unit test code coverage of 80%+ of sprint code
- Code - Most recent code pulled down from develop or release/prep (whichever is more current) and initial merge done (to size merge story for next sprint)
- Code - Short performance test run (poor results to be addressed in future sprint)
- Code - Static code scan pass
- Infrastructure – Clean vulnerability scan of third party libraries and supporting software
- QA - Automation scripts have a coverage of 80% of the sprint code

Release

- All sprints are complete as defined by the DoD for sprints
- All stories are complete and required bugs are fixed
- Full end to end regression testing complete
- No degradation in performance
- No security vulnerabilities in code, third party libraries or supporting software
- Documentation is complete and available
- Release deliverables are complete and available
- Non-functional requirements are complete (as defined by the project plan and release requirements)
- Code is passed to Customer Response team, after the project team has monitored the update in production for a minimum of 1 GA release
- The release is approved by the Release Committee

Incident Management

Auvik has a defined Security and Privacy Incident Management process to handle security and privacy incidents. This process can be initiated by an Auvik customer by contacting Auvik Technical Support, internal Auvik employee (via the above incident management process) or the public by emailing security@auvik.com.

In the event that a security incident is identified the following high-level process is followed.

- Monitoring and Awareness: A security and/or privacy incident is identified and communicated to the Security Incident Response Team (SIRT).
- Detection and Analysis (triage): The incident is assessed to determine the severity, priority, scope and impact. This step can include evidence preservation and containment activities.
- Mitigation: Recommendations are created and executed that will to contain, eradicate and/or recover from the incident in question.
- Recovery: Containment is complete. Where applicable, scanning of environments occurs to ensure mitigation is complete.
- Communications: This can include communications with internal resource teams, stakeholders and Auvik customers. Based on the findings of triage and analysis, the appropriate communications are drafted, approved and shared.
- Post Incident Activity: In this stage, lessons learned are completed to gather feedback and evolve incident response process and procedures. Where applicable, root cause is identified and logged.

Deficiency Reporting

Systems and processes are in place to support the identification, capture and exchange of information in a form and timeframe to allow people to carry out their responsibilities. This includes the ability of Auvik to perform the following:

- Initiate, record, process and report customer's transactions (as well as events and conditions) and maintain accountability for these.
- Provide an understanding of the individual roles and responsibilities pertaining to internal controls (including the extent to which Auvik understands how its activities relate to the work of others and their customers) and the means for reporting exceptions to higher management levels within Auvik and to customers.

Auvik provides various mechanisms for information sharing and communication with customers' employees and external parties. Examples of these mechanisms include:

Customers

- Problems with network connectivity (call, chat or email to Technical Support, Partner Success, etc.)
- Performance and availability
- Security or Privacy Incident
- GDPR Access Rights Request

Auvik initiated

- Proactive identification of problems
- Verification of customer's application status prior, during and after the implementation of a potential service-impacting change
- Advanced scheduling notification of potential service-impacting changes to customers.

Employees

- Corporate-wide Policies: Through Auvik's internal Wiki

External Parties

- Media communications: through Auvik's Marketing team, Blog, Slack, news and other information is communicated to external parties and posted on Auvik's external web

Risk Assessment

The goal of the risk assessment process is to identify, assess and evaluate relevant risks that could impact the achievement of the business objectives and develop responses to manage these risks. The outcome of a service organization's risk assessment process may affect the services provided to the service organization's customers. Information Security performs annual audits on selected risk assessment activities within the business units and/or the functional groups and provides recommendations for improvement. The results of the audits with the related management action plan are reported to the Security and Privacy Governance Committee (SPGC) and the Executive Management team.

The SPGC keeps abreast of the strategic and operational risks of the organization through the review and assessment of risks identified by the business units and functional groups through their engagement in the annual strategic business planning process.

Infrastructure

Elements of the data center such as cages, cabinets, cooling, power, humidity and fire suppression and physical security are monitored by the data center providers. The data center providers are responsible for maintaining these systems and ensuring that they are tested and functioning at all times. As a result, these systems are not in scope for Auvik in this report.

Environment and Procedural Controls

The infrastructure control environment reflects the overall awareness and actions of Auvik management concerning the internal controls of the Auvik Platform.

Auvik's operational policies and procedures are documented and are readily available to employees on the company Wiki. The responsibility and accountability for developing and maintaining these polices, and changes and updates to these policies are assigned to the appropriate Auvik personnel. Additionally, the information in these policies is reviewed on an annual basis by the appropriate Auvik employees. The information in these policies relates to the specific Common Criteria from the Security Trust Services Principles, covering the requirements of authorized users; assessing risks on a periodic basis; preventing unauthorized access; adding new users, modifying the access levels of existing users, and removing users who no longer need access; assigning responsibility and accountability for system availability and related security; assigning responsibility and accountability for system changes and maintenance; testing, evaluating, and authorizing system components before implementation; addressing how complaints and request relating to system availability and related security issues are resolved; identifying and mitigating system availability and related security breaches and other incidents; providing training and other resources to support the system availability and related security policies; providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies; recovering and continuing service in accordance with documented customer commitments or other agreements; and monitoring system capacity to achieve customer commitments or other agreements regarding availability.

Complementary User Entity Control Considerations

The Auvik Platform is designed with the assumption that certain controls would be implemented by customers. In certain situations, the implementation of specific controls by the customer is necessary to achieve control objectives included in this report.

This section describes additional controls that should be implemented by our customers to complement the controls at Auvik. User organizations should consider whether or not the following controls have been placed in operation at their organizations:

- Customer agrees that it and its end users will not use the network for illegal purposes, to infringe the rights of a third party, or to interfere with or disrupt the network.

- Customers are responsible for immediately notifying Auvik of any actual or suspected information security breaches, including compromised user accounts.
- Customer is responsible for ensuring that user endpoints are protected against viruses and malware and also any data files uploaded by a user to the client's application.
- Customers are responsible for using a supported browser configuration when accessing the Auvik Platform.
- Customers are responsible for providing up-to-date and valid information for Auvik Technical Support for the purposes of receiving updates to tickets, incidents, maintenance windows and other pertinent information.
- If maintaining their own authentication service, customers are responsible for:
    - Ensuring the authentication service is available.
    - Ensuring the password controls are appropriately set based on industry standards.
    - Ensuring MFA is configured for end users.

The list of user organization control considerations presented above do not represent a comprehensive set of all the controls that should be employed by our customers. Other controls may be required depending on the customer's configuration.

Complementary Subservice Organizations Controls

In providing services to its clients, Auvik utilizes the services of other organizations, collectively called subservice organizations. These organizations include, but are not limited to:

- Amazon Web Services: used to provide cloud hosting for our production environment.
- Salesforce: used to store customer contact information, subscription status, and other related information.
- Zuora: used to process e-subscription billing for Auvik customers.

Auvik undertakes to use a commercially reasonable selection process by which it evaluates the security, privacy, and confidentiality practices of proposed sub processors that will or may have access to or process Service Data.

Auvik requires its subservices to satisfy equivalent obligations as those required from Auvik (as a Data Processor) as set forth in Auvik's Terms of Service, including but not limited to the requirements to:

- process Personal Data in accordance with data controller's (i.e. Customer's) documented instructions (as communicated in writing to the relevant sub processor by Auvik).
- in connection with their sub processing activities, use only personnel who are reliable and subject to a contractually binding obligation to observe data privacy and security, to the extent applicable, pursuant to applicable data protection laws.
- provide regular training in security and data protection to personnel to whom they grant access to Personal Data.
- implement and maintain appropriate technical and organizational measures (including measures consistent with those to which Auvik is contractually committed to adhere insofar as they are equally relevant to the sub processor's processing of Personal Data on Auvik's behalf).
- promptly inform Auvik about any actual or potential security breach; and cooperate with Auvik in order to deal with requests from data controllers, data subjects, or data protection authorities, as applicable.

Auvik management monitors the subservice organization with periodic communication in relation to their ongoing processes including any exceptions reported. The sub-service organization relevant processes are audited routinely by random checks by Auvik for status updates and workflow consistency. Periodic reviews and quality assurance monitoring over the subservice organizations are conducted by Auvik.

Section IV: Trust Services Criteria, ISO 27001 Control and Related Management Controls

This section includes Information on the mapping of Auvik's Trust Services Criteria and related controls to ISO 27001 Controls Descriptions. Although the Trust Services Criteria and related controls are presented in this section, they are an integral part of Auvik's description of the system.

Trust Services Common Criteria 1 – Control Environment

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	5.1 A.7.2.1 A.7.2.2 A.7.2.3	Auvik has documented the code of business conduct and ethical standards which are reviewed, updated if applicable, and approved by senior management annually.
			Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers/business partners and all personnel, including contractors, are required to read and accept the code of business conduct and ethical standards upon their hire and formally reaffirm them annually thereafter.
			Management monitors personnel compliance with the code of business conduct and ethical standards through monitoring of customer and workforce member complaints and sanctions are applied to personnel who violate the code of business conduct.
			Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, criminal, employment checks and additionally credit checks for financial personnel.
			Before a third party is engaged by Auvik, the third-party personnel undergo background screening that includes, at a minimum, criminal, employment checks and additionally credit checks for financial consultants.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	5.1c 5.1h A.7.2.0	The Board of Directors are appointed to act on behalf of the shareholders and their roles and responsibilities as outlined in the Board of Directors' Charter are segregated from the roles and responsibilities of management.
			The Board of Directors' by-law includes the minimum background and skills required of Board of Directors. During the annual board meeting, the background and skills of each board member is compared to the background and skills noted in the Board of Directors' by-law.
			The Board of Directors' by-law includes the minimum background and skills required of Board of Directors and during the annual board meeting, the background and skills of each board member is compared to the background and skills noted in the Board of Directors' by-law.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			The Board of Directors consist of majority of independent members as per the Board of Directors' by-law to maintain independence from management.
			Auvik has a Security and Privacy committee that provides support to the Board of Directors.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	4.3 5.1 5.3 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4	Auvik's Management evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives.
			Job descriptions are reviewed by Auvik management on a semi-annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made to enable execution of authorities and responsibilities and flow of information to manage the activities of Auvik.
			Roles and responsibilities are defined in written job descriptions and communicated to managers taking into consideration segregation of duties as necessary at the various levels of the organization and requirements relevant to security.
			The management's security commitments and obligations are posted on Auvik's website. Roles and responsibilities for external party interaction and activity monitoring are defined in written job descriptions and communicated to personnel.
			Auvik's Management evaluate its sub processors as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	7.1 7.2 A.5.1.1 A.5.1.2 A.6.1.0 A.7.1.0 A.7.2.1	Roles and responsibilities are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated, for all employees, contractors and vendors, as part of the hiring or transfer evaluation process to support the achievement of objectives.
			Personnel competence across Auvik and in outsourced service providers is measured against established policies and practices as part of the semi-annual evaluation process or when new outsourced service provider relationships are established to support the achievement of Auvik's service commitments and system requirements. Any shortcomings noted during the evaluation are addressed with action items and re-evaluated in the following year's evaluation process or sooner.
			Management establishes requisite skillsets for personnel, whether an employee, contractor, or vendor employee, and provides continued training about its commitments and requirements for personnel to support the achievement of objectives. Management monitors compliance with training requirements.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			During its ongoing and periodic business planning, business continuity planning and budgeting process, management and the Board of Directors evaluate the need for additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.
			Prior to employment, personnel, including contractors and vendor employees, are verified against regulatory screening databases, including at a minimum, criminal, employment checks and additionally credit checks for financial personnel.
			The experience and training of candidates, whether an employee, contractor, or vendor employee, for employment of transfer are evaluated before they assume the responsibilities of their position to support the achievement of objectives. Existing personnel are evaluated at least annually.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A.6.1.0 A.7.2.3	During onboarding, new employees sign a letter to confirm they agree with, and will adhere to their role and responsibilities as articulated in the offer of employment.
			Management establish measurable goals and performance evaluation criteria, at all levels of Auvik, considering the achievement of both short-term and longer-term objectives.
			Management evaluate performance of internal control responsibilities, providing rewards and sanctions appropriate for responsibilities, considering the achievement of both short-term and longer-term objectives.

Trust Services Common Criteria 2 – Communication and Information

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A.8.2.1 A.8.2.2	Auvik performs assessment at least annually to identify the information required and expected to support the internal control and the achievement of Auvik service commitments and system requirements. Auvik most valuable and sensitive digital data and mission-critical systems, critical assets are identified during the assessment, including internal and external sources of data.
			Auvik has implemented various processes and procedures relevant to security to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	7.3 7.4 A.7.1.1 A.7.2.1 A.7.3.0 A.12.1.0 A.12.1.1 A.16.1.2 A.16.1.3 A.16.1.5 A.16.1.6	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, is provided to personnel to carry out their responsibilities.
			Auvik management and the Board of Directors meet quarterly and annually to communicate information needed to fulfill their roles with respect to the achievement of Auvik's service commitments and system requirements.
			Auvik has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management and the Board of Directors as necessary.
			Auvik has anonymous third-party hosted portal and shared mailbox available to internal and external users. Management monitors customer and workforce member complaints reported via this portal and shared mailbox.
			Auvik holds quarterly and annual board meetings. In addition, for communication of an unforeseen event, incident response policies and procedures are in place that includes escalation plan based on the nature and severity of the incident to senior management and the Board of Directors as necessary.
			Auvik's security commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities. The responsibilities of internal users whose roles affect system operation are communicated to those parties. Responsibilities and policies and procedures posted on Auvik's intranet are updated as necessary.
			Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			Changes to Auvik's commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose services are part of the system.
			Management provides continued training about its security commitments and requirements for personnel to support the achievement of objectives, and consistently monitors compliance with security training requirements. Auvik also provides user guides, security alerts and known issues on its websites and customer portal with information to improve security knowledge and awareness.
			Auvik's security commitments are communicated to external users, as appropriate. Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.
			Planned changes to system components are reviewed, scheduled, and communicated to management as part of the bi-weekly release process. These changes are communicated to external users via the Auvik's website.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	7.4 A.7.1.1 A.13.2.3 A.15.1.2 A.16.1.2	Auvik has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management, the Board of Directors and external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties as necessary.
			Auvik has made available contact email and phone numbers on its website and customer portal to customers, consumers, suppliers, external auditors, regulators, financial analysts, and others. Management monitors customer and workforce member complaints reported via the portals, emails and phones.
			Auvik meets with the Board of Directors quarterly to provide relevant information resulting from assessments conducted by internal and external parties. In addition, any significant information security related findings noted as part of Auvik's financial audits are communicated by the external auditor to the Audit Committee during quarterly and annual meetings.
			Auvik posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, and data on its intranet for internal users and on the internet for external users.
			Auvik security commitments are communicated to external users, as appropriate.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			Auvik changes to services that affect privacy and/or confidentiality are communicated to external users, as appropriate. Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities.
			Auvik posts a description of its system, upcoming releases, and upcoming maintenance on its public support site for external users.
			Auvik provides external users with access to multiple levels of support via their support portal and partner success program.

Trust Services Common Criteria 3 – Risk Assessment

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	6.2c 7.1 A.18.1.1 A.18.1.2	Auvik management performs a risk assessment annually, which is based on the objectives established by management under the oversight of the Board of Directors. These assessed risks are reviewed quarterly to identify changes in underlying threats or in the environment that would require an update to assessed risks.
			Auvik engages external legal service to identify changes to laws and regulations relating to Auvik services for the jurisdictions in which it operates.
			Auvik engages an external financial auditing service annually to ensure Auvik is following proper accounting practices.
			Reported changes from the external legal and financial services are evaluated by the Data Privacy Officer and CFO for their impact and the valuations are communicated to senior management and are incorporated into the risk assessment and review process.
			Auvik reviews its metrics and reporting quarterly to ensure its accuracy and relevance.
			Contracts personnel within finance maintain a database of contract terms and commitments. Updates of or modifications to standard contractual terms and commitments are approved by the CFO prior to contract approval and are incorporated into the risk assessment and review process.
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.	5.1c 6.1.1 6.1.2 6.1.2a 6.1.2b 6.1.2c 6.1.2d 6.1.2e 8.2 8.3 A.8.2.0 A.15.1.0 A.15.1.1 A.15.1.2	Auvik's Security and Privacy Committee meets every quarter to discuss strategy and operations, financial results, risk considerations, and other factors critical to the business.
			An annual risk assessment is performed to identify risks arising from external and internal sources and the effectiveness of these controls are shared with executive management and the audit committee.
			An overview of the annual risk assessment is presented to the audit committee and is used to help establish the annual audit plan.
			The information security team assess and responds to security risks on an ongoing basis through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			Auvik has a defined information classification scheme for the labeling and handling of data. Auvik classifies data into three levels: public, confidential, and strictly confidential.
			Auvik conducts an assessment of risk prior to the acquisition or outsourcing of third party services.
			A company-wide risk assessment is performed annually by management and includes the following: a. Determining business objectives, entity, subsidiary, division, operating unit, and functional levels. b. Evaluating the effect of environmental, regulatory, and technological changes on Auvik's system security c. Involving appropriate levels of management. d. Analyzing risks associated with the threats. e. Identifying threats to operations, including security threats, using Information Technology asset records. f. Identifying threats to operations, including threats from vendors, business partners, and other parties. Determining a risk mitigation strategy.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	6.1.2	Management conducts a periodic fraud risk assessment to identify the various ways that fraud and misconduct can occur, including how management might engage in inappropriate actions, and maintains documentation of this assessment.
			The board, audit committee and management review the Auvik's compensation and performance evaluation programs annually to identify potential incentives and pressures for employees to commit fraud.
			Auvik has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.
			Management uses information technology tools including security systems, fraud detection and monitoring systems, and incident tracking systems to identify and manage fraud risk.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A.12.1.1	Auvik evaluates changes in the regulatory, economic, and physical environment in which it operates, through the ongoing annual risk assessment process.
			Auvik evaluates changes in the business environment, including industry, competitors, regulatory environment, and consumers, through the ongoing annual risk assessment process.
			Auvik evaluates changes in the potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies, through the ongoing annual risk assessment process.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			Auvik evaluates changes in Auvik's systems and changes in the technology environment, through the ongoing annual risk assessment process.
			Auvik evaluates changes in vendor and business partner relationships, through the ongoing annual risk assessment process.

Trust Services Common Criteria 4 – Monitoring Activities

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
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.	7.2 9.1 9.2 9.3 10.2 A.18.2.0 A.18.2.1 A.18.2.2 A.18.2.3	The internal audit department performs periodic audits to include information security assessment.
			Internal audit annual plans include a risk analysis of all significant operating and reporting areas of Auvik as a means to prioritize audit efforts for the year.
			Auvik develops, documents, and maintains a baseline configuration of the internal control system provides training, and semi-annual performance reviews, for internal security personnel.
			On a quarterly basis, internal audit performs an assessment of the audit plan and scope to identify potential changes impacting Auvik's risk profile.
			An internal audit resource exists within information security team, reporting to the CFO.
			Internal audit personnel perform audit procedures using a formal methodology, document their procedures and results in working papers, and prepare an audit report summarizing the procedures performed and the findings from those procedures.
			Internal audit developed audit programs that include a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment process and various levels of management.
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.	9.1 9.2 9.2f 10.1d A.15.2.0 A.16.1.2 A.18.2.2 A.18.2.3	Complete reports of deficiencies in internal control from internal and external sources are provided to the board and audit committee. The board and audit committee work with management to suggest appropriate remediation and follow up to ensure that proper controls have been established.
			Auvik has established a practice that requires all deficiencies rated as serious threats to be reported to senior management and to the board or audit committee.
			Management tracks the status of all deficiencies that have been rated as a serious threat to the organization until satisfactorily resolved.

Trust Services Common Criteria 5 – Control Activities

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	6.1.3b 6.2 8.3 A.6.1.1	As part of its annual risk assessment, management maps identified risks to controls that have been designed and operated to address them. As new controls are identified, management develops the requirements and uses the change management process to implement them.
			As part of the risk assessment, management assesses the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks.
			When the management identifies a need for new controls, management considers a mix of control activities, including both manual/automated controls and preventive/detective controls.
			Auvik has designed application-enforced segregation of duties to define what privileges are assigned to users within applications.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	6.1.3b 8.3	As part of the corporate strategic plan, strategic risks affecting the organization and recommended courses of action are identified and discussed.
			Management develops a list of control activities to manage the technology infrastructure risks identified during the annual risk assessment process.
			Auvik employs organization-defined tailored acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	5.2 7.2 10.1a A.5.1.0 A.5.1.1 A.7.2.1	Auvik's policy and procedure manuals address controls over significant aspects of operations. Policy sections include • Security requirements for authorized users; • Data classification and associated protection, access rights, retention, and destruction requirements; • Risk assessment; • Access protection requirements; • User provisioning and de-provisioning; • Responsibility and accountability for security; • Responsibility and accountability for system changes and maintenance; • Change management; • Complaint intake and resolution; • Security and other incidents identification, response and mitigation; • Security training; • Handling of exceptions and situations not specifically addressed in policies; • Commitment and requirement identification and compliance measurement; and Information sharing and disclosure.
			The Auvik Security and Privacy Committee is charged with establishing, maintaining, and enforcing the overall security policies and procedures.
			Monthly service level assessments are performed by the functional heads of each department. These assessments include evaluation of the operation of key controls.
			Assessments are reviewed at quarterly at Auvik's Quarterly Business Review meetings and require the development of corrective action plans for control weaknesses.
			Auvik has written job descriptions specifying the responsibilities and the academic and professional requirements for key job positions. Human resources personnel screen internal and external job applicant qualifications based on the defined requirements within the job description.
			Auvik's policy and procedure manuals are reviewed annually by the Data Privacy Officer, Chief Financial Officer, and VP of Engineering for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.

Trust Services Common Criteria 6 – Logical and Physical Activity Controls

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
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.	A.8.1.1 A.8.1.2 A.9.1.1 A.9.2.2 A.9.2.6 A.9.3.0 A.9.4.1 A.9.4.2 A.9.4.3 A.10.1.0 A.10.1.1 A.18.1.4	Auvik monitors all system components through an automated management interface to log, track, and maintain all inventory components.
			Auvik permits remote access to production systems by authorized employees only with multifactor authentication (MFA) over a Secure Shell tunnel. Remote Access requires a change request which will deploy the temporary host.
			End user and server workload network traffic is segmented to support isolation.
			Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.
			A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. SSL certificates are used at the entry-point firewalls to information assets to establish access control rules.
			Passwords for in-scope system components are configured according to the Auvik's policy, which a. Requires fourteen-character minimum and 90-day password changes; b. Is complexity enabled; and Locks users out of the system after ten invalid attempts.
			The configuration management policy requires that all system changes undergo formal documentation, review, and authorization.
			Databases housing sensitive customer data are encrypted at rest.
			Encryption keys used by integrated services are encrypted themselves with a unique key.
CC6.2	Prior to issuing system credentials and granting system access, the entity	A.9.2.1 A.9.2.2 A.9.2.5	Access to in-scope system components requires a documented access request ticket and manager approval prior to access being provisioned.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
	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.	A.9.2.6	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.
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.	A.6.1.1 A.9.2.2 A.9.2.6	Asset owners periodically review access to ensure continued appropriateness.
			A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.
			Auvik establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles. Auvik tracks and monitors privileged role assignments on a continuous basis through automated mechanisms.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	A.8.1.3 A.8.3.0 A.9.2.2 A.9.2.4 A.9.2.6 A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.9	Access to the data centers requires a documented access request form and manager approval prior to access being provisioned.
			A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.
			Access to the data centers is reviewed quarterly by management.
CC6.5	The entity discontinues logical and physical	A.8.1.3 A.8.3.0	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
	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.	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.7	Prior to removal from company facilities, all digital media is completely degaussed and sanitized to remove any data and software.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A.13.1.1 A.13.1.2 A.13.1.3	System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined.
			The company has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information over public networks.
			Intrusion detection systems are used to provide continuous monitoring of the Auvik's network and prevention of potential security breaches.
			Auvik permits remote access to production systems by authorized employees only with multifactor authentication (MFA) over SSH.
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.	A.6.2.0 A.8.3.1 A.8.3.3 A.10.1.1 A.10.1.2 A.11.2.6 A.13.2.0 A.13.2.1 A.13.2.2 A.14.1.2 A.14.1.3	The information system restricts the ability of users to transmit, move, or remove system information to other information systems or networks.
			Secure file transfer protocols (SFTP) are deployed for transmission of confidential and/or sensitive information over public networks.
			Removable media to be used for customer or system data is encrypted and sanitized prior to connecting such devices to the information system.
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.	A.12.1.1 A.12.2.0 A.12.6.1 A.14.2.5	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software is explicitly covered in the employee Acceptable Use and Operational Controls policy.
			Auvik's build infrastructure and system management solution alerts system administrators of new software introduction into production.
			Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			Anti-malware technology is deployed for environments commonly susceptible to malicious attack. This software is used to scan assets prior to being placed into production.
			Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests.

Trust Services Common Criteria 7 – System Operations

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
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.	9.1 A.12.6.0	Baseline configurations are covered in the Operations controls policy document and are reviewed and updated annually. The configurations are updated when required due to reviews and system changes, and anytime integral system components are added.
			An infrastructure monitoring tool is utilized to monitor infrastructure availability and performance and generates alerts when specific predefined thresholds are met.
			Auvik utilizes a configuration monitoring tool that notifies management of changes to production system.
			Automated mechanisms are used to continuously detect the addition of unauthorized components/devices into the system. The configuration monitoring tool logs all changes in status to network switch ports. Any attempt to insert or install a component immediately sends an alert to the monitoring tool and creates a ticket.
			Internal and external network vulnerability scans are performed annually. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.
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.	A.12.4.1 A.12.4.3 A.16.1.2 A.16.1.3	User entities are provided with instructions for communicating potential security breaches to the information security team.
			When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.
			Security incidents are reported to the support and tracked through to resolution. Incidents that may affect security compliance are reported to Auvik's information security team.
			Intrusion detection systems are used to provide continuous monitoring of the Auvik's network and prevention of potential security breaches. All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.
CC7.3	The entity evaluates security events to	7.4 A.16.1.1	Auvik has developed security incident response policies and procedures that are communicated to authorized users.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
	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.	A.16.1.2 A.16.1.4 A.16.1.5	Auvik's security team is responsible for all incidents related to the security and monitor the logging, tracking, and communication to affected parties until resolved. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack.
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.	7.1 7.4 10.1 10.1e 10.2 A.16.1.1 A.16.1.3 A.16.1.5	Management has established defined roles and responsibilities to oversee implementation of information security policies including incident response.
			The containment phase ensures that all other interconnections to the system were not affected by the security incident.
			After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.
			An assessment of the incident response to better handle future incidents is performed through analysis after-action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.
			Daily encrypted backups are configured for all client data and stored for 14 days.
			AWS GuardDuty is used to provide continuous monitoring of the Auvik's network and prevention of potential security breaches.
			Internal and external network vulnerability scans are performed Annually. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.
			A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.4 10.1b A.16.1.4 A.16.1.6 A.17.1.1 A.17.1.2	Software updates related to flaw remediation are tested for effectiveness and potential side effects on the system before installation. All software updates and patches are tested by creating a virtual instance of the environment and running the tests associated with the re software update and/or patch. An ability to rollback is implemented during software updates and/or patching.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			The root cause determined by Auvik's information security team and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the procedures.
			Auvik incorporates lessons learned from ongoing incident response activities into incident response procedures accordingly. If changes are required, necessary changes are made to the policy and procedures and redistributed according to all responsible organizations and key personnel.
			Auvik has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning. Security administration team approval of changes is required prior to implementation.
			Annual testing of the incident response plan is performed using tabletop exercises and simulations to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned from tabletop exercises are used to implement changes to reflect effective procedures when handling incidents.

Trust Services Common Criteria 8 – Change Management

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
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.	7.5.3e A.12.1.1 A.12.5.0 A.13.2.3 A.14.1.0 A.14.2.1 A.14.2.2 A.14.2.3 A.14.2.5 A.14.2.7 A.14.2.8 A.14.2.9 A.14.3.0 A.18.1.3	Auvik has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.
			Auvik's software and infrastructure change management process requires that change requests are: a. Authorized b. Formally documented c. Tested prior to migration to production Reviewed and approved
			Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements.
			Auvik requires all changes, including maintenance activities, to be documented in Jira and tracked from initiation through deployment and validation.
			Internal and external network vulnerability scans are performed annually. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.
			Baseline configurations are retained within the configuration manager tool for roll back capability anytime an approved configuration change is made.
			Auvik maintains a documented change management process.
			Auvik utilizes real time detection of software vulnerabilities. A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum.
			Auvik contracts with third parties to conduct annual security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Management develops a plan of action for each recommendation and follows up on open recommendations monthly.
			Auvik prepares a root cause analysis for high severity incidents. Based on the root cause analysis, change requests are prepared, and Auvik's risk management process and relevant risk management data is updated to reflect the planned incident response.

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
			Auvik maintains a formally documented change management process. Changes to hardware, operating system, and system software are authorized, tested (when applicable), and approved by appropriate personnel prior to implementation.
			Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.
			Emergency changes follow the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented.

Trust Services Common Criteria 9 – Risk Mitigation

TSC #	Trust Services Criterion	ISO Ref.	Related Management Control
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	No reference	Auvik has a documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed.
			The risk management program includes the use of insurance to minimize the financial impact of any loss events.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	No reference	Formal information sharing agreements are in place with related parties and vendors. These agreements include the scope of services and security commitments applicable to that entity.
			A vendor risk assessment is performed for all vendors on an annual basis that have access to confidential data or impact the security of the system.
			Management has established defined roles and responsibilities to oversee implementation of information security policies.
			Auvik has clauses in its agreements with vendors and business partners to terminate relationships when necessary. Vendor and business partner access is removed upon termination through a termination checklist and access is revoked within 24 hours as part of the termination process.

Unmapped ISO 27001 Control Descriptions and Related Management Policy

ISO Ref.	ISO Controls	Related Auvik Policy
4.1	**Understanding the Organization and its context** The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].	Security and IT Objectives Security Incident Management Policy
4.2	**Understanding the needs and expectations of interested parties** The organization shall determine: a. Interested parties that are relevant to the information security management system; b. The requirements of these interested parties relevant to information security NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations	Operational Control Policy
4.4	**Information security management system** The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	Risk Assessment Process Operational Control Policy

ISO Ref.	ISO Controls	Related Auvik Policy
6.1.3	**Actions to address risks and opportunities** a. select appropriate information security risk treatment options, taking account of the risk assessment results; c. compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed. d. produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)), justification for their inclusion, whether the necessary controls are implemented or not; and the justification for excluding any of the Annex A controls. e. formulate an information security risk treatment plan; and f. obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process. NOTE The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000[5].	Risk Assessment Process
7.5.1	**General Documented Information** The organization's information security management system shall include: a. documented information required by this International Standard; b. documented information determined by the organization as being necessary for the effectiveness of the information security management system.	https://www.auvik.com/terms/ https://support.auvik.com/hc/en-us/sections/115001625203-2018-Product-Releases
7.5.2	**Creating and updating Documented Information** When creating and updating documented information the organization shall ensure appropriate: a. identification and description (e.g. a title, date, author, or reference number); b. format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c. review and approval for suitability and adequacy.	Code of Conduct Acceptance Personnel Security Policy

ISO Ref.	ISO Controls	Related Auvik Policy
8.1	**Operational planning and control** a. The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. b. The organization shall also implement plans to achieve information security objectives determined in 6.2. c. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. d. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. e. The organization shall ensure that outsourced processes are determined and controlled.	Operational Controls Policy
A.6.1.5	**Information security in project management** Information security shall be addressed in project management, regardless of the type of the project.	Security Incident Management Policy Security and Privacy Incident Management Process
A.6.2.2	**Teleworking** A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Access Audit Process Access Control Policy
A.8.1.3	**Acceptable use of assets** Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Personal Security Policy
A.8.2.3	**Handling of assets** Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Personal Security Policy
A.8.3.2	**Disposal of media** Media shall be disposed of securely when no longer required, using formal procedures.	Media Sanitization and Disposal Policy & Process
A.9.1.1	**Access control policy** An access control policy shall be established, documented and reviewed based on business and information security requirements.	Access Audit Process Access Control Policy
A.9.2.4	**Management of secret authentication information of users** The allocation of secret authentication information shall be controlled through a formal management process.	Access Control Policy
A.9.4.4	**Use of privileged utility programs** The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Access Control Policy

ISO Ref.	ISO Controls	Related Auvik Policy
A.9.4.5	**Access control to program source code** Access to program source code shall be restricted.	Access Control Policy
A.11.2.2	**Supporting utilities** Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Security and Privacy Incident Management Process
A.11.2.8	**Unattended user equipment** Users shall ensure that unattended equipment has appropriate protection.	Personal security policy
A.12.1.4	**Separation of development, testing and operational environments** Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Operational Control Policy
A.12.4.2	**Protection of log information** Logging facilities and log information shall be protected against tampering and unauthorized access.	Access Audit Process Access Control Policy
A.12.4.4	**Clock synchronization** The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	Operational Control Policy
A.12.7.1	**Information systems audit controls** Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Operational Control Policy Access Audit Process
A.13.2.3	**Electronic messaging** Information involved in electronic messaging shall be appropriately protected.	Personal Security Policy
A.14.2.4	**Restrictions on changes to software packages** Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Personal Security Policy
A.16.1.7	**Collection of evidence** The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Personal Security Policy

Section V: Mapping Trust Services Criteria to ISO 27001 Control Descriptions

Additional information on the mapping of Auvik's Trust Services Criteria and related controls to ISO 27001 Controls Descriptions are included in this section.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	5.1	**Leadership and Commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system
		A.7.2.1	**Management responsibilities** Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
		A.7.2.2	**Information Security awareness, education and training** All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
		A.7.2.3	**Disciplinary process** There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
CC1.2	COSO Principle 2: The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	5.1c	**Leadership and commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system by: c) ensuring that the resources needed for the information security management system are available
		5.1h	**Leadership and commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system by: Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility
		A.7.2.0	**Management responsibilities** Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	4.3	**Determining the scope of the information security management system** The organization shall determine the boundaries and applicability of the information security management system to establish its scope.
		5.1	**Leadership and Commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system
		5.3	**Organizational roles, responsibilities and authorities** Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.
		A.6.1.1	**Information security roles and responsibilities** All information security responsibilities shall be defined and allocated.
		A.6.1.2	**Segregation of duties** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
		A.6.1.3	**Contact with authorities** Appropriate contacts with relevant authorities shall be maintained.
		A.6.1.4	**Contact with special interest groups** Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	7.1	**Resources** The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		7.2	**Competence:** The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence.
		A.5.1.1	**Policies for information security** A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
		A.5.1.2	**Review of the policies for information security** The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		A.6.1.0	**Information security roles and responsibilities** All information security responsibilities shall be defined and allocated.
		A.7.1.0	**Screening** Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
		A.7.2.1	**Information Security awareness, education and training** All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their	A.6.1.0	**Information security roles and responsibilities** All information security responsibilities shall be defined and allocated.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
	internal control responsibilities in the pursuit of objectives.	A.7.2.3	**Disciplinary process** There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A.8.2.1	**Classification of information** Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
		A.8.2.2	**Labelling of information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	7.3	**Awareness** Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.
		7.4	**Communication** The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.
		A.7.1.1	**Terms and conditions of employment** The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.
		A.7.2.1	**Information Security awareness, education and training** All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.7.3.0	**Termination or change of employment responsibilities** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
		A.12.1.0	**Documented operating procedures** Operating procedures shall be documented and made available to all users who need them.
		A.12.1.1	**Change management** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled
		A.16.1.2	**Reporting information security events** Information security events shall be reported through appropriate management channels as quickly as possible.
		A.16.1.3	**Reporting information security weakness** Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
		A.16.1.5	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.
		A.16.1.6	**Learning from information security incidents** Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	7.4	**Communication** The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.
		A.7.1.1	**Terms and conditions of employment** The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.13.2.3	**Confidentiality or non- disclosure agreements** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
		A.15.1.2	**Information and communication technology supply chain** Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain
		A.16.1.2	**Reporting information security weakness** Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	6.2c	**Information security objectives and planning to achieve them** The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: c) take into account applicable information security requirements, and results from risk assessment and risk treatment
		7.1	**Resources** The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.
		A.18.1.1	**Identification of applicable legislation and contractual requirements** All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
		A.18.1.2	**Intellectual property rights** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
CC3.2	COSO Principle 7: 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.	5.1c	**Leadership and commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system by: c) ensuring that the resources needed for the information security management system are available
		6.1.1	**General** When planning for the information security management system, the organization shall consider the issues, risks and opportunities that need to be addressed.
		6.1.2	**Information Security risk assessment** The organization shall define and apply an information security risk assessment process that:
		6.1.2a	a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;
		6.1.2b	b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;
		6.1.2c	c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;
		6.1.2d	d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;
		6.1.2e	e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analyzed risks for risk treatment.
		8.2	**Information security risk assessment** The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		8.3	**Information security risk treatment** The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.
		A.8.2.0	**Classification of information** Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
		A.15.1.0	**Information security policy for supplier relationships** Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
		A.15.1.1	**Information security policy for supplier relationships** Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
		A.15.1.2	**Addressing security within supplier agreements** All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	6.1.2	**Information Security risk assessment** The organization shall define and apply an information security risk assessment process.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	A.12.1.1	**Change management** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	7.2	**Competence:** The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence.
		9.1	**Monitoring, measurement, analysis and evaluation** The organization shall evaluate the information security performance and the effectiveness of the information security management system.
		9.2	**Internal audit** The organization shall conduct internal audits at planned intervals to provide information on the information security management system.
		9.3	**Management review** Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
		10.2	**Continual improvement** The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.
		A.18.2.0	**Independent review of information security** The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.
		A.18.2.1	**Independent review of information security** The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.18.2.2	**Compliance with security policies and standards** Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
		A.18.2.3	**Technical compliance review** Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.
CC4.2	COSO Principle 17: 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.	9.1	**Monitoring, measurement, analysis and evaluation** The organization shall evaluate the information security performance and the effectiveness of the information security management system.
		9.2	**Internal audit** The organization shall conduct internal audits at planned intervals to provide information on the information security management system.
		9.2f	**Internal audit** The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: f) ensure that the results of the audits are reported to relevant management
		10.1d	**Nonconformity and corrective action** When a nonconformity occurs, the organization shall: d) review the effectiveness of any corrective action taken
		A.15.2.0	**Monitoring and review of supplier services** Organizations shall regularly monitor, review and audit supplier service delivery.
		A.16.1.2	**Reporting information security weakness** Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
		A.18.2.2	**Compliance with security policies and standards** Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
		A.18.2.3	**Technical compliance review** Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	6.1.3b	**Information security risk treatment** The organization shall define and apply an information security risk treatment process to: b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source.
		6.2	**Information security objectives and planning to achieve them** The organization shall establish information security objectives at relevant functions and levels.
		8.3	**Information security risk treatment** The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.
		A.6.1.1	**Segregation of duties** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	6.1.3b	**Information security risk treatment** The organization shall define and apply an information security risk treatment process to: b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source.
		8.3	**Information security risk treatment** The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.
CC5.3	COSO Principle 12: The entity deploys control activities through policies	5.2	**Policy** Top management shall establish an information security policy.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
	that establish what is expected and in procedures that put policies into action.	7.2	**Competence:** The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence.
		10.1a	**Nonconformity and corrective action** When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences
		A.5.1.0	**Policies for information security** A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
		A.5.1.1	**Review of the policies for information security** The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		A.7.2.1	**Information Security awareness, education and training** All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
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.	A.8.1.1	**Inventory of assets** Information, other assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
		A.8.1.2	**Ownership of assets** Assets maintained in the inventory shall be owned.
		A.9.1.1	**Access to networks and network services** Users shall only be provided with access to the network and net-work services that they have been specifically authorized to use.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.9.2.2	**User access provisioning** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
		A.9.2.6	**Removal or adjustment of access rights** The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
		A.9.3.0	**Use of secret authentication information** Users shall be required to follow the organization's practices in the use of secret authentication information.
		A.9.4.1	**Information access restriction** Access to information and application system functions shall be restricted in accordance with the access control policy.
		A.9.4.2	**Secure log-on procedures** Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
		A.9.4.3	**Password management system** Password management systems shall be interactive and shall ensure quality passwords.
		A.10.1.0	**Policy on the use of cryptographic controls** A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
		A.10.1.1	**Key management** A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
		A.18.1.4	**Regulation of cryptographic controls** Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
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	A.9.2.1	**User registration and de-registration** A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
		A.9.2.2	**User access provisioning** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
	whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	A.9.2.5	**Review of user access rights** Asset owners shall review users' access rights at regular intervals.
		A.9.2.6	**Removal or adjustment of access rights** The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
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.	A.6.1.1	**Segregation of duties** Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
		A.9.2.2	**Management of privileged access rights** The allocation and use of privileged access rights shall be restricted and controlled.
		A.9.2.6	**Removal or adjustment of access rights** The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	A.8.1.3	**Return of assets** All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
		A.8.3.0	**Management of removable media** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
		A.9.2.2	**User access provisioning** A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
		A.9.2.4	**Review of user access rights** Asset owners shall review users' access rights at regular intervals.
		A.9.2.6	**Removal or adjustment of access rights** The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.11.1.1	**Physical security perimeter** Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
		A.11.1.2	**Physical entry controls** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
		A.11.1.3	**Securing offices, rooms and facilities** Physical security for offices, rooms and facilities shall be designed and applied.
		A.11.1.5	**Working in secure areas** Procedures for working in secure areas shall be designed and applied.
		A.11.1.6	**Delivery and loading areas** Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
		A.11.2.1	**Equipment siting and protection** Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
		A.11.2.3	**Cabling security** Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
		A.11.2.5	**Removal of assets** Equipment, information or software shall not be taken off-site without prior authorization.
		A.11.2.6	**Security of equipment and assets off-premises** Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
		A.11.2.9	**Clear desk and clear screen policy** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the	A.8.1.3	**Return of assets** All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
	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.	A.8.3.0	**Management of removable media** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
		A.11.1.1	**Physical security perimeter** Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
		A.11.1.2	**Physical entry controls** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
		A.11.1.3	**Securing offices, rooms and facilities** Physical security for offices, rooms and facilities shall be designed and applied.
		A.11.1.5	**Working in secure areas** Procedures for working in secure areas shall be designed and applied.
		A.11.1.6	**Delivery and loading areas** Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
		A.11.2.1	**Equipment siting and protection** Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
		A.11.2.3	**Cabling security** Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
		A.11.2.5	**Removal of assets** Equipment, information or software shall not be taken off-site without prior authorization.
		A.11.2.6	**Security of equipment and assets off-premises** Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.11.2.7	**Secure disposal or re-use of equipment** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A.13.1.1	**Network controls** Networks shall be managed and controlled to protect information in systems and applications.
		A.13.1.2	**Security of network services** Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
		A.13.1.3	**Segregation in networks** Groups of information services, users and information systems shall be segregated on networks.
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.	A.6.2.0	**Mobile device policy** A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
		A.8.3.1	**Management of removable media** Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
		A.8.3.3	**Physical media transfer** Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
		A.10.1.1	**Policy on the use of cryptographic controls** A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
		A.10.1.2	**Key management** A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
		A.11.2.6	**Secure disposal or re-use of equipment** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.13.2.0	**Information transfer policies and procedures** Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
		A.13.2.1	**Information transfer policies and procedures** Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
		A.13.2.2	**Agreements on information transfer** Agreements shall address the secure transfer of business information between the organization and external parties.
		A.14.1.2	**Securing application services on public networks** Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
		A.14.1.3	**Protecting application services transactions** Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
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.	A.12.1.1	**Change management** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
		A.12.2.0	**Controls against malware** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
		A.12.6.1	**Restrictions on software installation** Rules governing the installation of software by users shall be established and implemented.
		A.14.2.5	**Secure development environment** Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to	9.1	**Monitoring, measurement, analysis and evaluation** The organization shall evaluate the information security performance and the effectiveness of the information security management system.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
	configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A.12.6.0	**Management of technical vulnerabilities** Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
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.	A.12.4.1	**Event logging** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
		A.12.4.3	**Administrator and operator logs** System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
		A.16.1.2	**Reporting information security events** Information security events shall be reported through appropriate management channels as quickly as possible.
		A.16.1.3	**Reporting information security weaknesses** Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
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.	7.4	**Communication** The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.
		A.16.1.1	**Responsibilities and procedures** Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
		A.16.1.2	**Reporting information security events** Information security events shall be reported through appropriate management channels as quickly as possible.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.16.1.4	**Assessment of and decision on information security events** Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
		A.16.1.5	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.
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.	7.1	**Resources** The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.
		7.4	**Communication** The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.
		10.1	**Nonconformity and corrective action**
		10.1e	**Nonconformity and corrective action** When a nonconformity occurs, the organization shall: e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered.
		10.2	**Continual improvement** The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.
		A.16.1.1	**Responsibilities and procedures** Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.16.1.3	**Assessment of and decision on information security events** Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
		A.16.1.5	**Response to information security incidents** Information security incidents shall be responded to in accordance with the documented procedures.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.4	**Communication** The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.
		10.1b	**Nonconformity and corrective action** When a nonconformity occurs, the organization shall: b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur
		A.16.1.4	**Assessment of and decision on information security events** Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
		A.16.1.6	**Learning from information security incidents** Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
		A.17.1.1	**Planning information security continuity** The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.17.1.2	**Implementing information security continuity** The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
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.	7.5.3e	**Control of documented information** Documented information required by the information security management system and by this International Standard shall be controlled to ensure: e) control of changes (e.g. version control)
		A.12.1.1	**Change management** Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled
		A.12.5.0	**Installation of software on operational systems** Procedures shall be implemented to control the installation of software on operational systems.
		A.13.2.3	**Confidentiality or non- disclosure agreements** Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
		A.14.1.0	**Information security requirements analysis and specification** The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
		A.14.2.1	**Secure development policy** Rules for the development of software and systems shall be established and applied to developments within the organization.
		A.14.2.2	**System change control procedures** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
		A.14.2.3	**Technical review of applications after operating platform changes** When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

TSC #	Trust Services Criterion	ISO Ref.	ISO Control Description
		A.14.2.5	**Secure development environment** Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
		A.14.2.7	**Outsourced development** The organization shall supervise and monitor the activity of out-sourced system development.
		A.14.2.8	**System security testing** Testing of security functionality shall be carried out during development.
		A.14.2.9	**System acceptance testing** Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
		A.14.3.0	**Protection of test data** Test data shall be selected carefully, protected and controlled.
		A.18.1.3	**Privacy and protection of personally identifiable information** Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.