ISO27001:2022 Readiness report for Polygraf Inc.

Generated on 28 January 2026

Report summary

This report provides a summary of Polygraf Inc.'s readiness posture for ISO27001:2022 compliance as of 28th January 2026. Sprinto continuously monitors the security and readiness posture of Polygraf Inc. to ensure you have a transparent view into how they have setup Sprinto to meet industry standards. Below is a list of controls implemented by the organization to meet the compliance requirements. Sprinto achieves this by connecting to the systems, tools and policies of the company, and running continuous checks to determine the health of the controls.

A.7

Physical Controls

A.7.1

Security perimeters should be defined and used to protect areas that contain information and other associated assets.

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

A.7.3

Physical security for offices, rooms and facilities should be designed and implemented

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

A.7.5

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

A.7.6

Security measures for working in secure areas should be designed and implemented.

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

A.7.7

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly

Staff devices should have screen lock enabled

Endpoint Security Policy

A.7.8

Equipment should be sited securely and protected.

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

A.7.9

Off-site assets should be protected.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly

Staff devices should have screen lock enabled

Endpoint Security Policy

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

Monitored via 3 checks

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Procedure

A.7.10

Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

A.7.11

Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

Monitored via 2 checks

Physical and Environmental Security Procedure

Physical & Environmental Security Policy

A.7.13

Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly

Staff devices should have screen lock enabled

Endpoint Security Policy

A.7.14

Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

C10

Improvement

C.10.1

When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management system, if necessary.

INTERNAL CONTROLS AND CHECKS

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

C.10.2

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

INTERNAL CONTROLS AND CHECKS

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C9

Performance evaluation

C.9.1

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.9.2

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization’s own requirements for its information security management system; and 2) the requirements of this International Standard; b) is effectively implemented and maintained.

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.9.3

Top management shall review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

INTERNAL CONTROLS AND CHECKS

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 26**

Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.

Monitored via 3 checks

Organization chart should be reviewed by senior management

HR Security Procedure

HR Security Policy

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management

Risk Assessment & Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

C8

Operation

C.8.1

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

INTERNAL CONTROLS AND CHECKS

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.8.2

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

C.8.3

The organization shall implement the information security risk treatment plan.

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

A.5

Organisational Controls

A.5.1

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

INTERNAL CONTROLS AND CHECKS

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

A.5.2

Information security roles and responsibilities should be defined and allocated according to the organization needs.

INTERNAL CONTROLS AND CHECKS

Control **SDC 2**

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

Monitored via 5 checks

Org chart should be maintained

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 3**

Entity has established procedures to communicate with staff about their roles and responsibilities.

Monitored via 3 checks

Organization roles and JDs should be validated

HR Security Procedure

HR Security Policy

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 154**

Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

Monitored via 1 check

Infrastructure operations person should be assigned

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

Monitored via 2 checks

People operations person should be assigned

HR Security Policy

Control **SDC 397**

Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.

Monitored via 3 checks

Compliance program manager should be assigned

Compliance Procedure

Compliance Policy

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

Monitored via 1 check

Organization of Information Security Policy

A.5.3

Conflicting duties and conflicting areas of responsibility should be segregated.

INTERNAL CONTROLS AND CHECKS

Control **SDC 2**

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

Monitored via 5 checks

Org chart should be maintained

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 3**

Entity has established procedures to communicate with staff about their roles and responsibilities.

Monitored via 3 checks

Organization roles and JDs should be validated

HR Security Procedure

HR Security Policy

Control **SDC 26**

Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.

Monitored via 3 checks

Organization chart should be reviewed by senior management

HR Security Procedure

HR Security Policy

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

Monitored via 1 check

Organization of Information Security Policy

A.5.4

Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured

HR Security Policy

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

A.5.5

The organization should establish and maintain contact with relevant authorities

INTERNAL CONTROLS AND CHECKS

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

Monitored via 1 check

Organization of Information Security Policy

A.5.6

The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.

INTERNAL CONTROLS AND CHECKS

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

Monitored via 1 check

Organization of Information Security Policy

A.5.7

Information relating to information security threats should be collected and analysed to produce threat intelligence.

INTERNAL CONTROLS AND CHECKS

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

Monitored via 4 checks

Health of production infrastructure should be monitored

Errors on production infrastructure should be monitored

Operation Security Policy

Operations Security Procedure

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 3 checks

Audit logs should exist

Operation Security Policy

Operations Security Procedure

A.5.8

Information security should be integrated into project management.

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

A.5.9

An inventory of information and other associated assets, including owners, should be developed and maintained.

INTERNAL CONTROLS AND CHECKS

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

Monitored via 1 check

Public access for infra assets should be restricted

Control **SDC 52**

Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

Monitored via 1 check

Critical Infrastructure assets should be identified

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 389**

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

Monitored via 3 checks

Internal Audit

Asset Management Policy

Asset Management Procedure

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

Monitored via 3 checks

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Procedure

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 5 checks

Deny by default firewall ruleset should be set up on all production hosts

Infrastructure provider should be configured

Asset Management Policy

Network Security Procedure

Asset Management Procedure

A.5.10

Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.

INTERNAL CONTROLS AND CHECKS

Control **SDC 105**

Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.

Monitored via 1 check

Acceptable Usage Policy

A.5.11

Personnel and other interested parties as appropriate should return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement.

INTERNAL CONTROLS AND CHECKS

Control **SDC 395**

Entity has documented policies and procedures to facilitate the implementation of personnel security.

Monitored via 2 checks

HR Security Procedure

HR Security Policy

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

Monitored via 2 checks

People operations person should be assigned

HR Security Policy

A.5.12

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

INTERNAL CONTROLS AND CHECKS

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

Monitored via 1 check

Data Classification Policy

Control **SDC 52**

Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

Monitored via 1 check

Critical Infrastructure assets should be identified

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

Monitored via 3 checks

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Procedure

Control **SDC 389**

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

Monitored via 3 checks

Internal Audit

Asset Management Policy

Asset Management Procedure

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 382**

Entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.

Monitored via 1 check

Data Classification Policy

A.5.13

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

INTERNAL CONTROLS AND CHECKS

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

Monitored via 1 check

Data Classification Policy

Control **SDC 69**

Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems

Monitored via 1 check

Information Security Policy

Control **SDC 52**

Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

Monitored via 1 check

Critical Infrastructure assets should be identified

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

Monitored via 3 checks

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Procedure

Control **SDC 389**

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

Monitored via 3 checks

Internal Audit

Asset Management Policy

Asset Management Procedure

A.5.14

Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

Monitored via 2 checks

Production systems should be secured with HTTPS

SSL connection should be enforced for servers

A.5.15

Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

INTERNAL CONTROLS AND CHECKS

Control **SDC 105**

Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.

Monitored via 1 check

Acceptable Usage Policy

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

Monitored via 3 checks

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Procedure

Control **SDC 389**

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

Monitored via 3 checks

Internal Audit

Asset Management Policy

Asset Management Procedure

A.5.16

The full life cycle of identities should be managed

INTERNAL CONTROLS AND CHECKS

Control **SDC 28**

Entity's Infosec officer reviews and approves the list of people with access to production console annually

Monitored via 1 check

Access to critical systems should be reviewed

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 4 checks

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

A.5.17

Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 135**

Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.

Monitored via 3 checks

Access Control Procedure

Acceptable Usage Policy

Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 4 checks

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism

Critical systems should be protected with a secure login mechanism

Access Control Procedure

Access Control Policy

A.5.18

Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 4 checks

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

A.5.19

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 1 check

Vendor Management Policy

A.5.20

Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 1 check

Vendor Management Policy

A.5.21

Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management

Risk Assessment & Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 1 check

Vendor Management Policy

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

A.5.22

The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

A.5.23

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization’s information security requirements.

INTERNAL CONTROLS AND CHECKS

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

Monitored via 1 check

Vendor Management Policy

A.5.24

The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

INTERNAL CONTROLS AND CHECKS

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 2 checks

Essential Contacts should be configured for the organization

Information Security Policy

Control **SDC 16**

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

Monitored via 1 check

Customer support page should be available

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

Monitored via 1 check

Threat detection system should be enabled

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

A.5.25

The organization should assess information security events and decide if they are to be categorized as information security incidents.

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

A.5.26

Information security incidents should be responded to in accordance with the documented procedures.

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 3 checks

Audit logs should exist

Operation Security Policy

Operations Security Procedure

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

Monitored via 1 check

Threat detection system should be enabled

A.5.27

Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

A.5.28

The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

Monitored via 1 check

Threat detection system should be enabled

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 3 checks

Audit logs should exist

Operation Security Policy

Operations Security Procedure

A.5.29

The organization should plan how to maintain information security at an appropriate level during disruption.

INTERNAL CONTROLS AND CHECKS

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

Control **SDC 60**

Entity tests backup information periodically to verify media reliability and information integrity.

Monitored via 1 check

Data backup restoration

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

A.5.30

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements

INTERNAL CONTROLS AND CHECKS

Control **SDC 60**

Entity tests backup information periodically to verify media reliability and information integrity.

Monitored via 1 check

Data backup restoration

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

Monitored via 1 check

Disaster recovery

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

Monitored via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

A.5.31

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization’s approach to meet these requirements should be identified, documented and kept up to date.

INTERNAL CONTROLS AND CHECKS

Control **SDC 386**

Entity maintains a list of legal, statutory, and regulatory requirements relevant to information security.

Monitored via 4 checks

Legal, statutory, regulatory and contractual requirements should be reviewed

Compliance Procedure

Compliance Policy

Information Security Policy

Control **SDC 431**

Entity has established policies and procedures to help identify and deal with legal, regulatory, and contractual compliance including facilitating relevant audits to review compliance status.

Monitored via 2 checks

Compliance Procedure

Compliance Policy

A.5.32

The organization should implement appropriate procedures to protect intellectual property rights.

INTERNAL CONTROLS AND CHECKS

Control **SDC 431**

Entity has established policies and procedures to help identify and deal with legal, regulatory, and contractual compliance including facilitating relevant audits to review compliance status.

Monitored via 2 checks

Compliance Procedure

Compliance Policy

A.5.33

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

Control **SDC 69**

Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems

Monitored via 1 check

Information Security Policy

Control **SDC 382**

Entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.

Monitored via 1 check

Data Classification Policy

Control **SDC 431**

Entity has established policies and procedures to help identify and deal with legal, regulatory, and contractual compliance including facilitating relevant audits to review compliance status.

Monitored via 2 checks

Compliance Procedure

Compliance Policy

A.5.34

The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

INTERNAL CONTROLS AND CHECKS

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy

Control **SDC 431**

Entity has established policies and procedures to help identify and deal with legal, regulatory, and contractual compliance including facilitating relevant audits to review compliance status.

Monitored via 2 checks

Compliance Procedure

Compliance Policy

Control **SDC 433**

Entity has documented policy and procedures which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations.

Monitored via 1 check

Privacy By Design Policy

A.5.35

The organization’s approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 431**

Entity has established policies and procedures to help identify and deal with legal, regulatory, and contractual compliance including facilitating relevant audits to review compliance status.

Monitored via 2 checks

Compliance Procedure

Compliance Policy

A.5.36

Compliance with the organization’s information security policy, topic-specific policies, rules and standards should be regularly reviewed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 431**

Entity has established policies and procedures to help identify and deal with legal, regulatory, and contractual compliance including facilitating relevant audits to review compliance status.

Monitored via 2 checks

Compliance Procedure

Compliance Policy

A.5.37

Documented operating procedures - Operating procedures for information processing facilities should be documented and made available to personnel who need them.

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management

Risk Assessment & Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

Monitored via 3 checks

Vendor risk assessment should be reviewed by senior management

Vendor Management Policy

Vendor Management Procedure

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 32**

Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.

Monitored via 4 checks

Org chart should be maintained

Compliance Procedure

Compliance Policy

Information Security Policy

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

A.8

Technological Controls

A.8.2

The allocation and use of privileged access rights should be restricted and managed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 4 checks

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

Monitored via 8 checks

Access to critical systems should be reviewed

IAM users should be assigned roles with least access

Policies should be attached to groups and should not be attached to users

Users of critical system should be identified

Accounts should not have admin privileges

Cloud storage buckets should have uniform bucket-level access enabled

Access Control Procedure

Access Control Policy

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism

Critical systems should be protected with a secure login mechanism

Access Control Procedure

Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

A.8.3

Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 4 checks

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

Monitored via 8 checks

Access to critical systems should be reviewed

IAM users should be assigned roles with least access

Policies should be attached to groups and should not be attached to users

Users of critical system should be identified

Accounts should not have admin privileges

Cloud storage buckets should have uniform bucket-level access enabled

Access Control Procedure

Access Control Policy

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism

Critical systems should be protected with a secure login mechanism

Access Control Procedure

Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

Monitored via 1 check

Public access for infra assets should be restricted

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 5 checks

Deny by default firewall ruleset should be set up on all production hosts

Infrastructure provider should be configured

Asset Management Policy

Network Security Procedure

Asset Management Procedure

A.8.4

Read and write access to source code, development tools and software libraries should be appropriately managed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism

Critical systems should be protected with a secure login mechanism

Access Control Procedure

Access Control Policy

A.8.5

Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.

INTERNAL CONTROLS AND CHECKS

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism

Critical systems should be protected with a secure login mechanism

Access Control Procedure

Access Control Policy

A.8.6

The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

INTERNAL CONTROLS AND CHECKS

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

Monitored via 1 check

Threat detection system should be enabled

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 3 checks

Audit logs should exist

Operation Security Policy

Operations Security Procedure

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

Monitored via 3 checks

Health of production infrastructure should be monitored

Asset Management Policy

Asset Management Procedure

A.8.7

Protection against malware should be implemented and supported by appropriate user awareness.

INTERNAL CONTROLS AND CHECKS

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

A.8.8

Information about technical vulnerabilities of information systems in use should be obtained, the organization’s exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.

INTERNAL CONTROLS AND CHECKS

Control **SDC 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

Monitored via 2 checks

Vulnerability should be closed in SLA

Vulnerability scanner should be enabled

Control **SDC 56**

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

Monitored via 1 check

Vulnerability should be closed in SLA

Control **SDC 63**

Entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.

Monitored via 1 check

VAPT exercise should be conducted annually

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

Monitored via 4 checks

Health of production infrastructure should be monitored

Errors on production infrastructure should be monitored

Operation Security Policy

Operations Security Procedure

A.8.9

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

Monitored via 3 checks

Health of production infrastructure should be monitored

Asset Management Policy

Asset Management Procedure

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

Monitored via 5 checks

Backup should be enabled on production database

Versioning should be enabled for storage assets

Operation Security Policy

Business Continuity Plan

Operations Security Procedure

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 4 checks

Data at rest should be encrypted

Encryption Policy

Asset Management Policy

Asset Management Procedure

A.8.10

Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

Monitored via 1 check

Data Retention Policy

A.8.20

Networks and network devices should be secured, managed and controlled to protect information in systems and applications.

INTERNAL CONTROLS AND CHECKS

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 5 checks

Deny by default firewall ruleset should be set up on all production hosts

Infrastructure provider should be configured

Asset Management Policy

Network Security Procedure

Asset Management Procedure

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism

Critical systems should be protected with a secure login mechanism

Access Control Procedure

Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

Monitored via 1 check

Public access for infra assets should be restricted

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

Monitored via 2 checks

Production systems should be secured with HTTPS

SSL connection should be enforced for servers

Control **SDC 119**

Entity has documented guidelines to manage communications protections and network security of critical systems.

Monitored via 2 checks

Communications & Network Security Policy

Network Security Procedure

A.8.11

Data masking should be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

INTERNAL CONTROLS AND CHECKS

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 4 checks

Data at rest should be encrypted

Encryption Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

Monitored via 2 checks

Production systems should be secured with HTTPS

SSL connection should be enforced for servers

Control **SDC 106**

Entity has a documented policy to manage encryption and cryptographic protection controls.

Monitored via 1 check

Encryption Policy

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy

A.8.12

Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

Monitored via 1 check

Data Protection Policy

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 4 checks

Data at rest should be encrypted

Encryption Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

Monitored via 2 checks

Production systems should be secured with HTTPS

SSL connection should be enforced for servers

Control **SDC 106**

Entity has a documented policy to manage encryption and cryptographic protection controls.

Monitored via 1 check

Encryption Policy

A.8.13

Backup copies of information, software and systems should be maintained and regularly tested inaccordance with the agreed topic-specific policy on backup.

INTERNAL CONTROLS AND CHECKS

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

Monitored via 5 checks

Backup should be enabled on production database

Versioning should be enabled for storage assets

Operation Security Policy

Business Continuity Plan

Operations Security Procedure

Control **SDC 60**

Entity tests backup information periodically to verify media reliability and information integrity.

Monitored via 1 check

Data backup restoration

A.8.14

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

INTERNAL CONTROLS AND CHECKS

Control **SDC 58**

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

Monitored via 5 checks

Backup should be enabled on production database

Versioning should be enabled for storage assets

Operation Security Policy

Business Continuity Plan

Operations Security Procedure

A.8.15

Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

Monitored via 1 check

Threat detection system should be enabled

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 3 checks

Audit logs should exist

Operation Security Policy

Operations Security Procedure

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

A.8.16

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

INTERNAL CONTROLS AND CHECKS

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

Monitored via 1 check

Threat detection system should be enabled

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

Monitored via 3 checks

Audit logs should exist

Operation Security Policy

Operations Security Procedure

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

Monitored via 4 checks

Health of production infrastructure should be monitored

Errors on production infrastructure should be monitored

Operation Security Policy

Operations Security Procedure

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

Monitored via 3 checks

Data Breach Notification Policy

PHI Data breach Notification Procedure

Personal Data Breach Notification Procedure

A.8.19

Procedures and measures should be implemented to securely manage software installation on operational systems.

INTERNAL CONTROLS AND CHECKS

Control **SDC 105**

Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.

Monitored via 1 check

Acceptable Usage Policy

Control **SDC 69**

Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems

Monitored via 1 check

Information Security Policy

A.8.21

Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.

INTERNAL CONTROLS AND CHECKS

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

Monitored via 3 checks

Health of production infrastructure should be monitored

Asset Management Policy

Asset Management Procedure

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

Monitored via 4 checks

Health of production infrastructure should be monitored

Errors on production infrastructure should be monitored

Operation Security Policy

Operations Security Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

Monitored via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 121**

Entity maintains network architecture diagrams that are accurate, up-to-date, and contain sufficient detail to assess the security of the network and document all sensitive/regulated data flows.

Monitored via 1 check

System architecture diagram

A.8.22

Groups of information services, users and information systems should be segregated in the organization’s networks.

INTERNAL CONTROLS AND CHECKS

Control **SDC 52**

Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

Monitored via 1 check

Critical Infrastructure assets should be identified

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

A.8.23

Access to external websites should be managed to reduce exposure to malicious content.

INTERNAL CONTROLS AND CHECKS

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly

Staff devices should have screen lock enabled

Endpoint Security Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

A.8.24

Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.

INTERNAL CONTROLS AND CHECKS

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

Monitored via 4 checks

Data at rest should be encrypted

Encryption Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 106**

Entity has a documented policy to manage encryption and cryptographic protection controls.

Monitored via 1 check

Encryption Policy

A.8.25

Rules for the secure development of software and systems should be established and applied.

INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured

HR Security Policy

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

A.8.26

Information security requirements should be identified, specified and approved when developing or acquiring applications.

INTERNAL CONTROLS AND CHECKS

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured

HR Security Policy

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

Monitored via 2 checks

Vulnerability should be closed in SLA

Vulnerability scanner should be enabled

Control **SDC 56**

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

Monitored via 1 check

Vulnerability should be closed in SLA

A.8.27

Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.

INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured

HR Security Policy

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

A.8.28

Secure coding principles should be applied to software development.

INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured

HR Security Policy

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 56**

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

Monitored via 1 check

Vulnerability should be closed in SLA

Control **SDC 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

Monitored via 2 checks

Vulnerability should be closed in SLA

Vulnerability scanner should be enabled

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

A.8.29

To validate if information security requirements are met when applications or code are deployed to the production environment.

INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

A.8.34

Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 63**

Entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.

Monitored via 1 check

VAPT exercise should be conducted annually

A.8.18

The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.

INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

A.8.1

Information stored on, processed by or accessible via user endpoint devices should be protected.

INTERNAL CONTROLS AND CHECKS

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly

Staff devices should have screen lock enabled

Endpoint Security Policy

A.8.30

The organization should direct, monitor and review the activities related to outsourced system development.

INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

A.8.31

Development, testing and production environments should be separated and secured.

INTERNAL CONTROLS AND CHECKS

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

A.8.32

Changes to information processing facilities and information systems should be subject to change management procedures.

INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

A.8.33

Test information should be appropriately selected, protected and managed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

Monitored via 4 checks

SDLC Procedure

Operation Security Policy

Operations Security Procedure

System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 5 checks

Change management repos should be classified

Change management source should be configured

SDLC Procedure

Operation Security Policy

Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

Monitored via 5 checks

Changes to production code should be reviewed by peers

Change requests should be reviewed by peers

SDLC Procedure

Operation Security Policy

Operations Security Procedure

C5

Leadership

C.5.1

Top management shall demonstrate leadership and commitment with respect to the information security management system

INTERNAL CONTROLS AND CHECKS

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 2 checks

Essential Contacts should be configured for the organization

Information Security Policy

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.5.2

Top management shall establish an information security policy

INTERNAL CONTROLS AND CHECKS

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

C.5.3

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

INTERNAL CONTROLS AND CHECKS

Control **SDC 2**

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

Monitored via 5 checks

Org chart should be maintained

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 3**

Entity has established procedures to communicate with staff about their roles and responsibilities.

Monitored via 3 checks

Organization roles and JDs should be validated

HR Security Procedure

HR Security Policy

Control **SDC 397**

Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.

Monitored via 3 checks

Compliance program manager should be assigned

Compliance Procedure

Compliance Policy

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

Monitored via 2 checks

People operations person should be assigned

HR Security Policy

Control **SDC 154**

Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

Monitored via 1 check

Infrastructure operations person should be assigned

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C4

Context of the organization

C.4.1

Understanding the organization and its context

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.4.2

Understanding the needs and expectations of interested parties

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

C.4.3

Determining the scope of the information security management system

INTERNAL CONTROLS AND CHECKS

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 2 checks

Essential Contacts should be configured for the organization

Information Security Policy

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

C.4.4

Establish, implement, maintain and continually improve information security management system

INTERNAL CONTROLS AND CHECKS

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 2 checks

Essential Contacts should be configured for the organization

Information Security Policy

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

A.6

People Controls

A.6.1

Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

INTERNAL CONTROLS AND CHECKS

Control **SDC 5**

Entity has established procedures to perform security risk screening of individuals before authorizing access.

Monitored via 2 checks

HR Security Procedure

HR Security Policy

A.6.2

The employment contractual agreements should state the personnel’s and the organization’s responsibilities for information security.

INTERNAL CONTROLS AND CHECKS

Control **SDC 2**

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

Monitored via 5 checks

- Org chart should be maintained
- HR Security Procedure
- Access Control Procedure
- HR Security Policy
- Access Control Policy

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

Monitored via 1 check

- Code of Business Conduct Policy

Control **SDC 3**

Entity has established procedures to communicate with staff about their roles and responsibilities.

Monitored via 3 checks

- Organization roles and JDs should be validated
- HR Security Procedure
- HR Security Policy

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

Monitored via 3 checks

Health of production infrastructure should be monitored

Asset Management Policy

Asset Management Procedure

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

Monitored via 2 checks

People operations person should be assigned

HR Security Policy

Control **SDC 395**

Entity has documented policies and procedures to facilitate the implementation of personnel security.

Monitored via 2 checks

HR Security Procedure

HR Security Policy

A.6.3

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

INTERNAL CONTROLS AND CHECKS

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

Monitored via 2 checks

Security training provider should be configured

HR Security Policy

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

A.6.4

A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

INTERNAL CONTROLS AND CHECKS

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

Monitored via 1 check

Code of Business Conduct Policy

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control **SDC 13**

Entity makes all policies and procedures available to all staff members for their perusal.

Monitored via 3 checks

ISMS Information Security Roles & Responsibilities

ISMS Manual

ISMS Scope Document

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

A.6.5

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.

INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

A.6.6

Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

Monitored via 1 check

Policies should be reviewed by senior management

A.6.7

Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.

INTERNAL CONTROLS AND CHECKS

Control **SDC 28**

Entity's Infosec officer reviews and approves the list of people with access to production console annually

Monitored via 1 check

Access to critical systems should be reviewed

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

Monitored via 4 checks

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

Monitored via 6 checks

User access to critical system should be validated by roles

Role based access should be setup

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

Monitored via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

Monitored via 8 checks

Access to critical systems should be reviewed

IAM users should be assigned roles with least access

Policies should be attached to groups and should not be attached to users

Users of critical system should be identified

Accounts should not have admin privileges

Cloud storage buckets should have uniform bucket-level access enabled

Access Control Procedure

Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

Monitored via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

Monitored via 4 checks

Access should be protected with secure login mechanism

Critical systems should be protected with a secure login mechanism

Access Control Procedure

Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

Monitored via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified

Access Control Procedure

Access Control Policy

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

Monitored via 5 checks

Staff devices should have antivirus running

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

Monitored via 2 checks

Staff devices should have disk encryption enabled

Endpoint Security Policy

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

Monitored via 5 checks

Staff devices should have OS updated

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

Monitored via 3 checks

Staff devices health should be monitored regularly

Staff devices should have screen lock enabled

Endpoint Security Policy

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

Monitored via 1 check

Media Disposal Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

Monitored via 3 checks

Endpoint Security Policy

Asset Management Policy

Asset Management Procedure

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

Monitored via 5 checks

Deny by default firewall ruleset should be set up on all production hosts

Infrastructure provider should be configured

Asset Management Policy

Network Security Procedure

Asset Management Procedure

A.6.8

The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

INTERNAL CONTROLS AND CHECKS

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 2 checks

Essential Contacts should be configured for the organization

Information Security Policy

Control **SDC 16**

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

Monitored via 1 check

Customer support page should be available

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

Monitored via 2 checks

Incident Management Procedure

Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

Monitored via 1 check

Incidents should be investigated based on severity

C6

Planning

C.6.1

Actions to address risk and opportunities

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

Monitored via 1 check

Risk assessment should be conducted periodically

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

Monitored via 1 check

Risk Assessment & Management Policy

C.6.2

Information security objectives and planning to achieve them

INTERNAL CONTROLS AND CHECKS

Control **SDC 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

Monitored via 1 check

Information security officer should be assigned

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 25**

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

Monitored via 4 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance Policy

Compliance Procedure

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

C.6.3

Planning of changes - When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

INTERNAL CONTROLS AND CHECKS

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

C7

Support

C.7.1

The organization shall determine and provide the resources needed for the establishment and maintenance of the information security management system.

INTERNAL CONTROLS AND CHECKS

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

Monitored via 2 checks

Risk assessment should be reviewed by senior management

Risk Assessment & Management Policy

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

Monitored via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 398**

Entity has a documented ISMS scope that defines which information and information assets the organization intends to protect.

Monitored via 4 checks

ISMS Scope Document

Compliance Procedure

Compliance Policy

Information Security Policy

C.7.2

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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 3**

Entity has established procedures to communicate with staff about their roles and responsibilities.

Monitored via 3 checks

Organization roles and JDs should be validated

HR Security Procedure

HR Security Policy

Control **SDC 2**

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

Monitored via 5 checks

Org chart should be maintained

HR Security Procedure

Access Control Procedure

HR Security Policy

Access Control Policy

Control **SDC 4**

Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.

Monitored via 2 checks

HR Security Procedure

HR Security Policy

Control **SDC 5**

Entity has established procedures to perform security risk screening of individuals before authorizing access.

Monitored via 2 checks

HR Security Procedure

HR Security Policy

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 9**

Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.

Monitored via 3 checks

Staff Performance Evaluations

HR Security Procedure

HR Security Policy

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control **SDC 13**

Entity makes all policies and procedures available to all staff members for their perusal.

Monitored via 3 checks

ISMS Information Security Roles & Responsibilities

ISMS Manual

ISMS Scope Document

Control **SDC 395**

Entity has documented policies and procedures to facilitate the implementation of personnel security.

Monitored via 2 checks

HR Security Procedure

HR Security Policy

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

Monitored via 3 checks

Infosec training should be completed by onboarded staff

HR Security Procedure

HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

Monitored via 2 checks

Infosec training should be completed by onboarded staff

Staff should periodically complete security training

C.7.3

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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

Monitored via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

Monitored via 2 checks

Policies should be acknowledged by onboarded staff

Staff should periodically acknowledge policies

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.7.4

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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

Monitored via 2 checks

Essential Contacts should be configured for the organization

Information Security Policy

Control **SDC 16**

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

Monitored via 1 check

Customer support page should be available

Control **SDC 13**

Entity makes all policies and procedures available to all staff members for their perusal.

Monitored via 3 checks

ISMS Information Security Roles & Responsibilities

ISMS Manual

ISMS Scope Document

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

Control **SDC 14**

Entity displays the most current information about its services on its website, which is accessible to its customers.

Monitored via 1 check

Product marketing website should be available

C.7.5.1

The organization’s information security management system shall include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary or the effectiveness of the information security management system.

INTERNAL CONTROLS AND CHECKS

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

Monitored via 1 check

Internal Audit

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.7.5.2

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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

C.7.5.3

Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

INTERNAL CONTROLS AND CHECKS

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

Monitored via 1 check

Org policy should be defined

Control **SDC 399**

Entity has a documented ISMS Manual which provides a framework that the organization can use to develop, implement, and maintain an effective information security management system.

Monitored via 5 checks

Compliance Procedure

Compliance Policy

Information Security Policy

ISMS Information Security Roles & Responsibilities

ISMS Manual

About Sprinto

Sprinto is a modern platform for continuous compliance monitoring. It automates the detection, remediation, and management of security risks, ensuring ongoing compliance with leading security and privacy standards.