SOC 2 Readiness report for AssistNow Inc

Generated on 11 February 2025

Report summary

This report provides a summary of AssistNow Inc's readiness posture for SOC 2 compliance as of 11th February 2025. Sprinto continuously monitors the security and readiness posture of AssistNow 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.

Legend

- Check is healthy
- Check is work in progress

A1

Additional Criteria for Availability

A1.2

The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

INTERNAL CONTROLS AND CHECKS

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 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 3 checks

Operation Security Policy	✓
Business Continuity Plan	✓
Operations Security Procedure	✓

A1.3

The entity tests recovery plan procedures supporting system recovery to meet its objectives.

INTERNAL CONTROLS AND CHECKS

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	✓

A1.1

The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

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 2 checks

Operation Security Policy	✓

Operations Security Procedure

CC1

Control Environment

CC1.1

COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

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 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 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 432

Entity outlines and documents cybersecurity responsibilities for all personnel.

Monitored via 1 check

Organization of Information Security Policy

CC1.5

COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

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 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 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

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

CC1.3

COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

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	✓
Access Control Procedure	✓
HR Security 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 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 Policy	✓
Compliance Procedure	✓

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 3 checks

Management Review of Internal Audit	✓
Senior management should be assigned	✓
Compliance Policy	✓

CC1.2

COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

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 3 checks

Management Review of Internal Audit

Senior management should be assigned

Compliance 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 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

CC1.4

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

INTERNAL CONTROLS AND CHECKS

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 3 checks

Hiring evaluation of new employee should be recorded

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 3 checks

Background checks should be conducted for new employees

HR Security Procedure

HR Security Policy

CC2

Communication and Information

CC2.2

COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

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 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

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 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 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 1 check

Information Security Policy

CC2.1

COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

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 2 checks

Asset Management Policy ✓

Asset Management Procedure ✓

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 ✓

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 71**

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

Monitored via 1 check

Data Retention Policy ✓

CC2.3

COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

INTERNAL CONTROLS AND CHECKS

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 ✓

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 ✓

CC3

Risk Assessment

CC3.2

COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

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 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 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

CC3.4

COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

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 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	✓

CC3.1

COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

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	✓

CC3.3

COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

INTERNAL CONTROLS AND CHECKS

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

CC4

Monitoring Activities

CC4.1

COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

INTERNAL CONTROLS AND CHECKS

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 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 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 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 3 checks

Management Review of Internal Audit ✓

Senior management should be assigned ✓

Compliance 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 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 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	✓

CC4.2

COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

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 1 check

Information 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 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 3 checks

Management Review of Internal Audit	✓
Senior management should be assigned	✓
Compliance Policy	✓

CC5

Control Activities

CC5.3

COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

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 developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined 

CC5.1

COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

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 31

Entity has developed a set of policies 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 Policy

Compliance Procedure

Information Security Policy

CC5.2

COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

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 3 checks

Management Review of Internal Audit ✓

Senior management should be assigned ✓

Compliance 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 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 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 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 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Monitored via 1 check

Org policy should be defined	✓

CC6

Logical and Physical Access Controls

CC6.7

The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

INTERNAL CONTROLS AND CHECKS

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

Monitored via 2 checks

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

Control **SDC 141**

Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.

Monitored via 7 checks

Staff devices should have disk encryption enabled

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Acceptable Usage 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 3 checks

Asset Management Policy

Asset Management Procedure

Encryption 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 1 check

Production systems should be secured with HTTPS

CC6.1

The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

INTERNAL CONTROLS AND CHECKS

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

Monitored via 3 checks

Access to critical systems should be reviewed	✓
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 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	✓
Access Control Procedure	✓
HR Security 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	✓

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	✓

CC6.6

The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

INTERNAL CONTROLS AND CHECKS

Control **SDC 141**

Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.

Monitored via 7 checks

Staff devices should have disk encryption enabled	✓
Staff devices health should be monitored regularly	⏱
Endpoint Security Policy	✓

Asset Management Policy

Physical and Environmental Security Procedure

Asset Management Procedure

Acceptable Usage 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 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 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 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 3 checks

Asset Management Policy	✓
Network Security Procedure	✓

Asset Management Procedure

Control SDC 119

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

Monitored via 2 checks

Network Security Procedure

Communications & Network Security Policy

CC6.2

Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

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	✓
Access Control Procedure	✓
HR Security 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 5 checks

Offboarded staff access to critical systems should be revoked	✓
Access Control Procedure	✓
HR Security Procedure	✓
HR Security Policy	✓
Access Control Policy	✓

CC6.3

The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving

consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

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	
Access Control Procedure	
HR Security 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 5 checks

Offboarded staff access to critical systems should be revoked	
Access Control Procedure	
HR Security 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 4 checks

Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓
Access Control Procedure	✓
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 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

CC6.8

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.

INTERNAL CONTROLS AND CHECKS

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 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 3 checks

Asset Management Policy

Network Security Procedure

Asset Management Procedure

CC6.5

The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.

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

CC7

System Operations

CC7.5

The entity identifies, develops, and implements activities to recover from identified security incidents.

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 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

CC7.1

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

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 2 checks

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 394**

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

Monitored via 2 checks

Operation Security Policy	✓
Operations Security Procedure	✓

CC7.2

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

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 2 checks

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 394**

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

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

CC7.3

The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

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 2 checks

Operation Security Policy

Operations Security 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

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 394**

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

Monitored via 2 checks

Operation Security Policy

Operations Security 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 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 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 112**

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

Monitored via 3 checks

Data Breach Notification Policy	✓
Personal Data Breach Notification Procedure	✓
PHI Data breach Notification Procedure	✓

CC7.4

The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

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 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 ✓

CC8

Change Management

CC8.1

The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

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

Monitored via 4 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓
System Acquisition and Development Lifecycle Policy	✓

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 66**

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

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

CC9

Risk Mitigation

CC9.1

The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

INTERNAL CONTROLS AND CHECKS

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 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 ✓

CC9.2

The entity assesses and manages risks associated with vendors and business partners.

INTERNAL CONTROLS AND CHECKS

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 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 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

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	✓

C1

Additional Criteria for Confidentiality

C1.1

The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

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 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 3 checks

Asset Management Policy	✓
Asset Management Procedure	✓
Encryption 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 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

C1.2

The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

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

PI1

Additional Criteria for Processing integrity

PI1.1

The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.

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

PI1.2

The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.

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

PI1.3

The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.

INTERNAL CONTROLS AND CHECKS

Control **SDC 66**

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

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 118**

Company does application regression testing to validate key processing for the application during the change management process.

Monitored via 2 checks

Operation Security Policy	✓
Operations Security Procedure	✓

PI1.4

The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.

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	✓
Access Control Procedure	✓
HR Security Procedure	✓
HR Security Policy	✓
Access Control Policy	✓

Control **SDC 66**

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

Monitored via 3 checks

Operation Security Policy	✓
SDLC Procedure	✓
Operations Security Procedure	✓

Control **SDC 118**

Company does application regression testing to validate key processing for the application during the change management process.

Monitored via 2 checks

Operation Security Policy

Operations Security Procedure

PI1.5

The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.

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 49**

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

Monitored via 3 checks

Asset Management Policy

Asset Management Procedure

Encryption Policy

P1

Additional Criteria for Privacy

P1.1

The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy 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 ✓

P1.0

Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

INTERNAL CONTROLS AND CHECKS

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

P2

Privacy Criteria Related to Choice and Consent

P2.1

The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

INTERNAL CONTROLS AND CHECKS

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control SDC 98

Entity maintains a list of all contractual obligations based on customer contracts.

Monitored via 1 check

Management review of contractual obligations

P3

Privacy Criteria Related to Collection

P3.1

Personal information is collected consistent with the entity’s objectives related to privacy.

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 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

P3.2

For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control SDC 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control SDC 76

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

P4

Privacy Criteria Related to Use, Retention, and Disposal

P4.1

The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

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	✓
Access Control Procedure	✓
HR Security Procedure	✓
HR Security Policy	✓
Access Control Policy	✓

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map	✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy	✓

P4.2

The entity retains personal information consistent with the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control SDC 71

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

Monitored via 1 check

Data Retention Policy

Control SDC 75

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

P4.3

The entity securely disposes of personal information to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control SDC 71

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

Monitored via 1 check

Data Retention Policy 

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map 

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy 

P5

Privacy Criteria Related to Access

P5.1

The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

P5.2

The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓

Vendor Management Policy ✓

Control SDC 80

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report ✓

Control SDC 144

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy ✓

P6

Privacy Criteria Related to Disclosure and Notification

P6.1

The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity’s objectives related to privacy.

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 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

Monitored via 1 check

Risk assessment should be conducted periodically 

P6.2

The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map 

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report 

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

P6.3

The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

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 112**

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

Monitored via 3 checks

Data Breach Notification Policy

Personal Data Breach Notification Procedure

PHI Data breach Notification Procedure

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity	✓
Incident Management Procedure	✓
Incident Management Policy	✓

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned	✓

Control **SDC 1105**

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

Monitored via 1 check

Personal Data Breach Notification Procedure	✓

P6.4

The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

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 2 checks

Vendor Management Policy	✓
Vendor Management Procedure	✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

P6.5

The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.

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 1 check

Information Security Policy ✓

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

Monitored via 2 checks

Vendor risk assessment should be conducted periodically ✓
Vendor Management Policy ✓

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner ✓

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

Monitored via 2 checks

Vendor risk assessment should be conducted periodically	✓
Vendor Management Policy	✓

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity	✓
Incident Management Procedure	✓
Incident Management Policy	✓

P6.6

The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

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 1 check

Information Security 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 112**

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

Monitored via 3 checks

Data Breach Notification Policy ✓

Personal Data Breach Notification Procedure ✓

PHI Data breach Notification Procedure ✓

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

Monitored via 3 checks

Incidents should be investigated based on severity ✓

Incident Management Procedure ✓

Incident Management Policy ✓

Control **SDC 1105**

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

Monitored via 1 check

Personal Data Breach Notification Procedure

P6.7

The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

P7

Privacy Criteria Related to Quality

P7.1

The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.

INTERNAL CONTROLS AND CHECKS

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

Monitored via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

Monitored via 1 check

Privacy officer should be assigned

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

Monitored via 1 check

Review of the privacy policy

P8

Privacy Criteria Related to Monitoring and Enforcement

P8.1

The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.

INTERNAL CONTROLS AND CHECKS

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

Monitored via 1 check

Data consent using cookie banner

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

Monitored via 1 check

Data Subject Access Requests (SARs) Report

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.