## E B THREE, LLC's SOC 2 Compliance Checklist

## **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



**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** 



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** 





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** 





**SDC 60** 

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

## Monitored via 1 check

Data backup restoration



## 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 4 checks

<b>✓</b>
<b>✓</b>
<b>✓</b>
<b>✓</b>

## A1.3

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

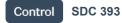
## INTERNAL CONTROLS AND CHECKS



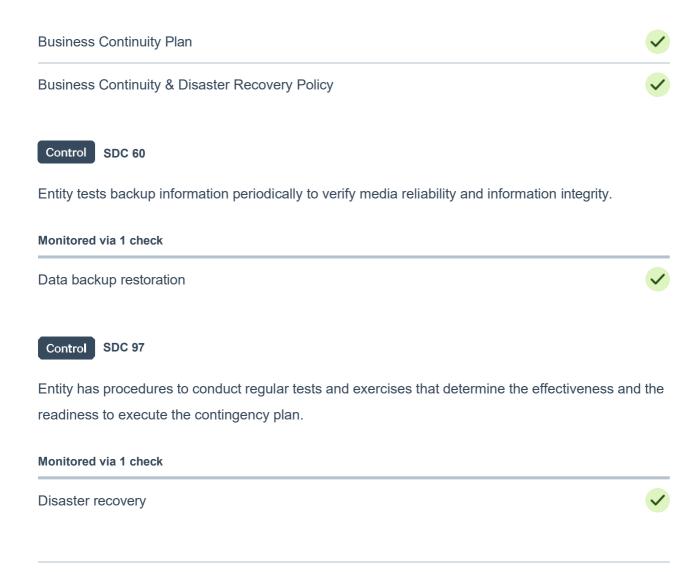
Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

## Monitored via 2 checks





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



## CC1

## **Control Environment**

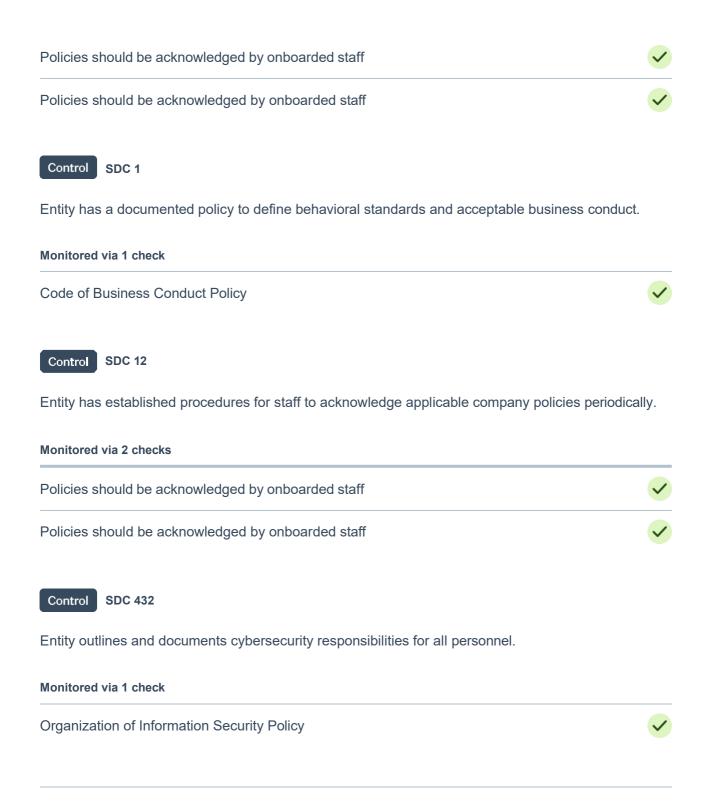
## CC1.1

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

## INTERNAL CONTROLS AND CHECKS



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



## 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 4 checks





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	<b>✓</b>
HR Security Procedure	<b>✓</b>
HR Security Policy	<b>✓</b>

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

## **CC1.3**

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

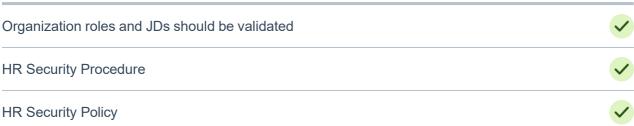
Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

## Monitored via 5 checks

Org chart should be maintained

HR Security Procedure	<b>✓</b>
Access Control Procedure	<b>✓</b>
HR Security Policy	<b>✓</b>
Access Control Policy	<b>✓</b>
Control SDC 3	
Entity has established procedures to communicate with staff about their roles and responsibilities	S.

## Monitored via 3 checks





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



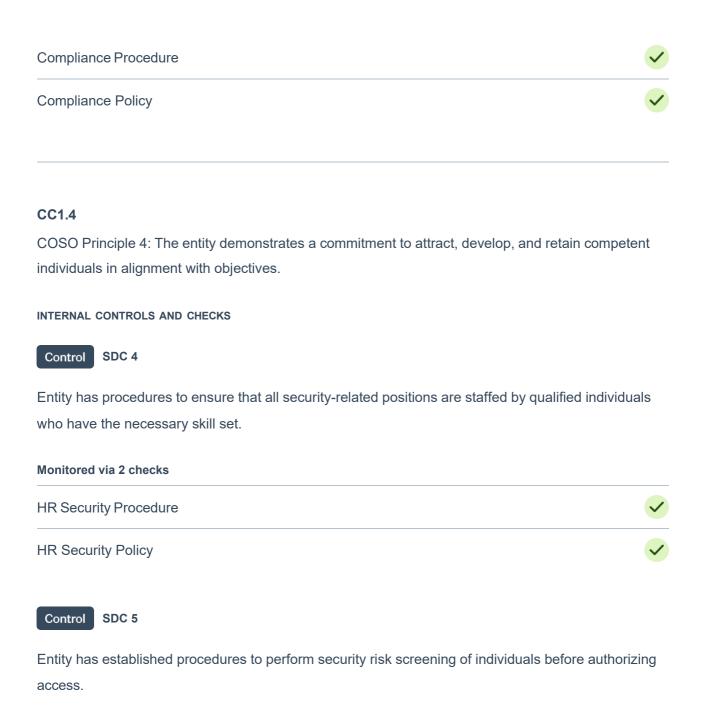


Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

## Monitored via 1 check

Infrastructure operations person should be assigned **SDC 396** Control 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 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



## Monitored via 2 checks

HR Security Procedure	<b>✓</b>
HR Security Policy	<b>~</b>

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

## INTERNAL CONTROLS AND CHECKS



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** 



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





**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

# Control SDC 388 Entity documents, monitors, and retains individual training activities and records. Monitored via 1 check Infosec training should be completed 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

## CC2

## **Communication and Information**

## CC2.1

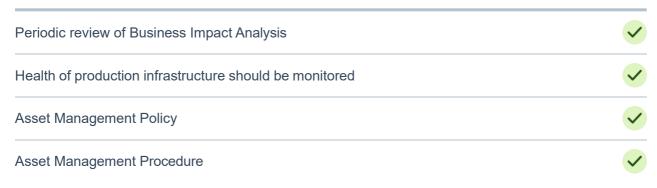
COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

## INTERNAL CONTROLS AND CHECKS



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

## Monitored via 4 checks





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** 





**SDC 71** 

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

## Monitored via 1 check

**Data Retention Policy** 



## 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



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

## Monitored via 2 checks

Policies should be acknowledged by onboarded staff



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 1 check

Infosec training should be completed 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



Policies should be acknowledged by onboarded staff



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



## CC2.3

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

INTERNAL CONTROLS AND CHECKS



**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**

## CC3.1

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



**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



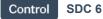
Risk Assessment & Management Policy



## CC3.2

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



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

## Monitored via 2 checks

Policies should be acknowledged by onboarded staff



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





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



## CC3.3

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

## INTERNAL CONTROLS AND CHECKS



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



## CC3.4

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

## INTERNAL CONTROLS AND CHECKS



**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



## 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



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 6 checks

Internal Audit	<b>✓</b>
Change management source should be configured	<b>✓</b>
Infrastructure provider should be configured	<b>✓</b>
Staff devices health should be monitored regularly	<b>✓</b>
Asset Management Policy	<b>✓</b>
Asset Management Procedure	<b>✓</b>



**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





**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	<b>✓</b>
Senior management should be assigned	<b>✓</b>
Compliance Procedure	<b>✓</b>
Compliance Policy	<b>✓</b>



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

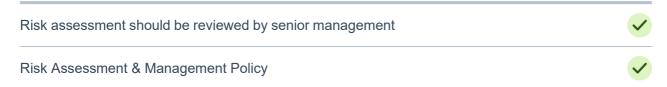
## Monitored via 3 checks

Organization chart should be reviewed by senior management	<b>✓</b>
HR Security Procedure	<b>✓</b>
HR Security Policy	<b>✓</b>



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

## Monitored via 2 checks





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

## Monitored via 3 checks





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



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





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

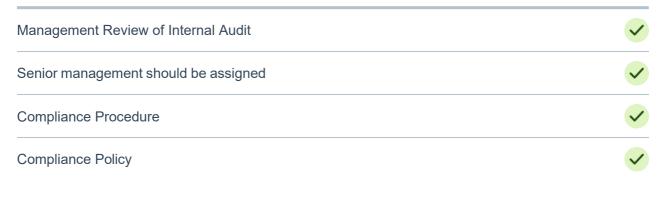


Control

**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



## CC5

## **Control Activities**

## 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



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 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



## CC5.2

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

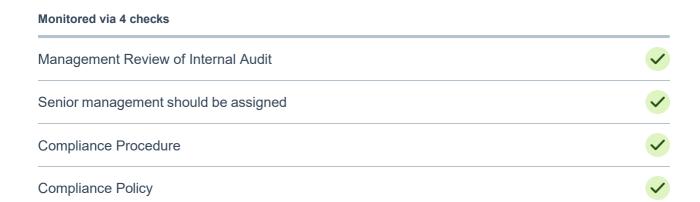
## INTERNAL CONTROLS AND CHECKS



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

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.



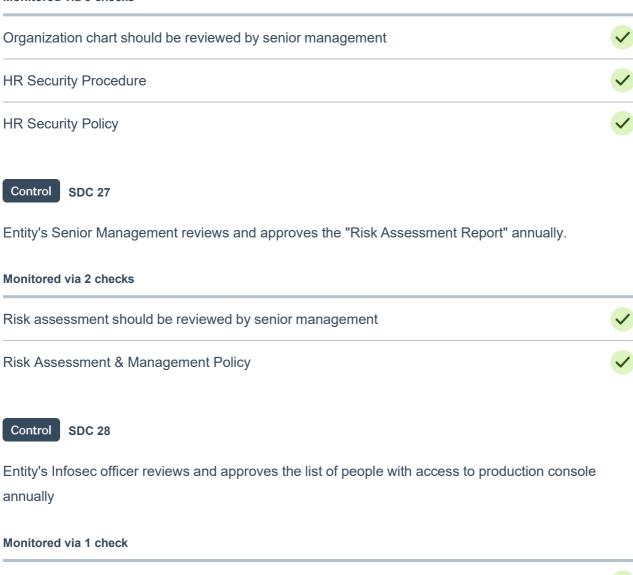


Control

**SDC 25** 

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

## Monitored via 3 checks





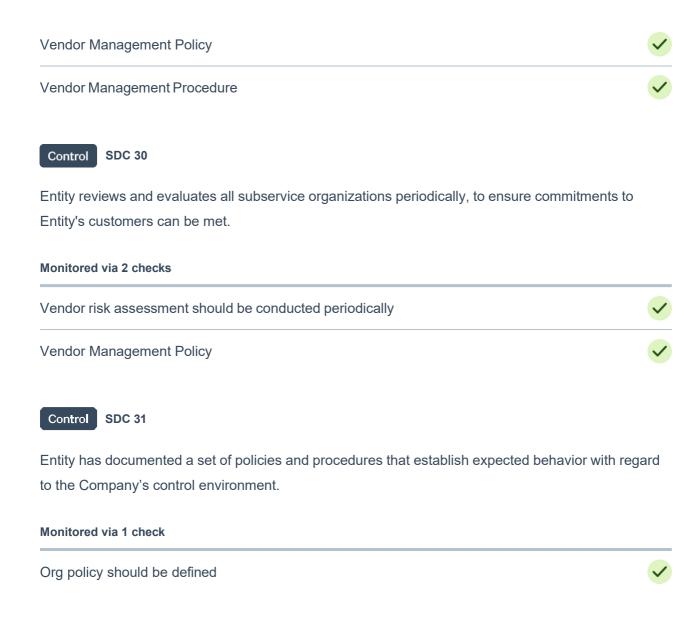
Access to critical systems should be reviewed

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





## 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



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

## Monitored via 2 checks

Policies should be acknowledged by onboarded staff



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



Policies should be acknowledged by onboarded staff



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



## CC6

## **Logical and Physical Access Controls**

## CC6.1

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

## INTERNAL CONTROLS AND CHECKS



**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

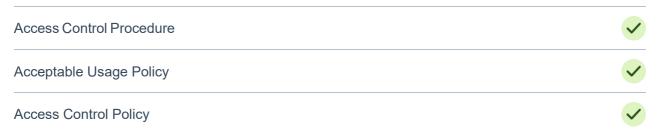




**SDC 135** 

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





**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.

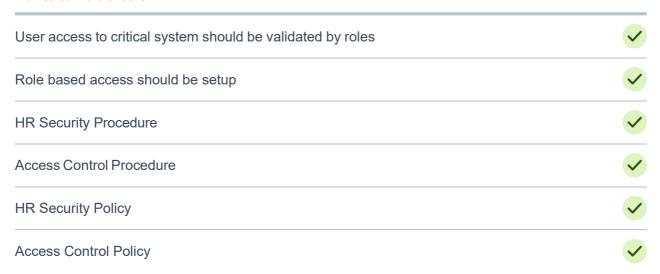
## Monitored via 2 checks





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



## 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 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 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	<b>✓</b>
Users of critical system should be identified	<b>✓</b>
Access Control Procedure	<b>✓</b>
Access Control Policy	V

## Control

## **SDC 381**

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

## Monitored via 2 checks





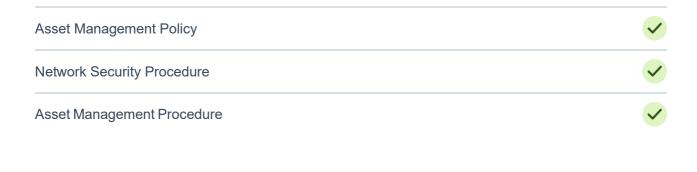
## **SDC 50**

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



## 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



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





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	<b>✓</b>
HR Security Procedure	<b>✓</b>
Access Control Procedure	<b>✓</b>
HR Security Policy	<b>✓</b>
Access Control Policy	<b>✓</b>

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	<b>✓</b>
Access Control Procedure	<b>✓</b>
HR Security Policy	<b>✓</b>
Access Control Policy	<b>✓</b>

## 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



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	<b>✓</b>
Role based access should be setup	<b>✓</b>
HR Security Procedure	<b>✓</b>
Access Control Procedure	<b>✓</b>
HR Security Policy	<b>✓</b>
Access Control Policy	<b>✓</b>

## Control SDC 35

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

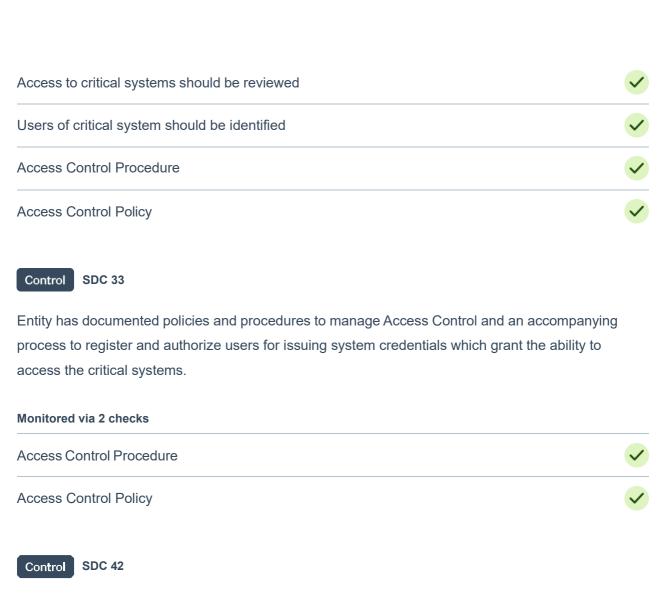
## Monitored via 4 checks





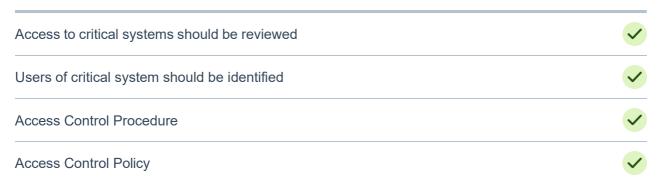
Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

## Monitored via 4 checks



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





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	<b>✓</b>
Users of critical system should be identified	<b>✓</b>
Access Control Procedure	<b>✓</b>
Access Control Policy	<b>✓</b>

# 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



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

### Monitored via 1 check



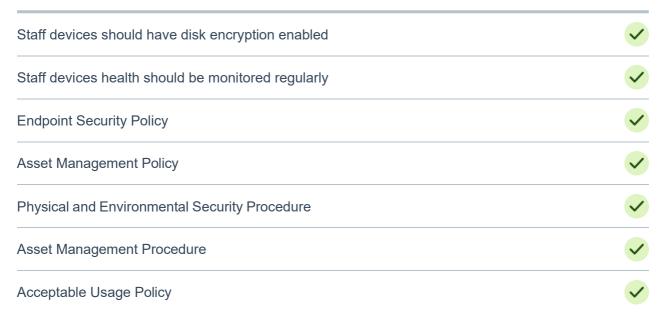
# **CC6.6**

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

Control SDC 141

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

# Monitored via 7 checks





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

# Monitored via 3 checks

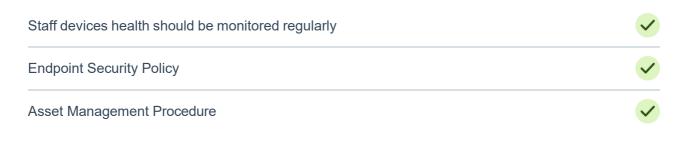




**SDC 390** 

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

# Monitored via 3 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 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 5 checks

Access should be protected with secure login mechanism	<b>✓</b>
Login protection methods for critical system related to Al	<b>✓</b>
Critical systems should be protected with a secure login mechanism	<b>✓</b>
Access Control Procedure	<b>✓</b>
Access Control Policy	<b>✓</b>

# 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 4 checks

Endpoint Security Policy	<b>✓</b>
Asset Management Policy	<b>✓</b>
Physical and Environmental Security Procedure	<b>✓</b>
Asset Management Procedure	<b>✓</b>

# Control SD

**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 3 checks

Staff devices should have disk encryption enabled	<b>✓</b>
Staff devices should have disk encryption enabled	<b>✓</b>
Endpoint Security Policy	<b>✓</b>

# 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	<b>✓</b>
Endpoint Security Policy	<b>✓</b>
Asset Management Policy	<b>✓</b>
Physical and Environmental Security Procedure	<b>✓</b>
Asset Management Procedure	<b>✓</b>

# 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.

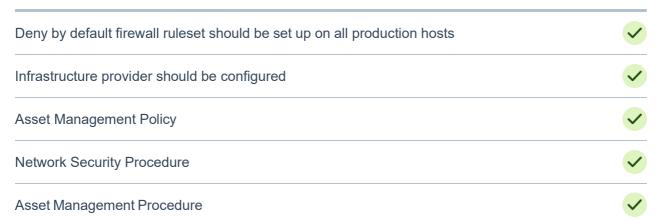
# Monitored via 3 checks

Staff devices health should be monitored regularly	<b>✓</b>
Staff devices should have screen lock enabled	<b>✓</b>
Endpoint Security Policy	<b>✓</b>

# 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





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

# Monitored via 2 checks

Communications & Network Security Policy



# 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



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

# Monitored via 3 checks

Critical Infrastructure assets should be identified **Asset Management Policy** Asset Management Procedure



**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 3 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 custon data at rest.  Monitored via 5 checks  Data at rest should be encrypted	
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 3 checks  Staff devices should have disk encryption enabled  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 custon data at rest.  Monitored via 5 checks	ld have disk encryption enabled
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 3 checks  Staff devices should have disk encryption enabled  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 custon data at rest.  Monitored via 5 checks	h should be monitored regularly
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 3 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 custon data at rest.  Monitored via 5 checks	Policy
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 3 checks  Staff devices should have disk encryption enabled  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 custon data at rest.  Monitored via 5 checks	at Policy
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 3 checks  Staff devices should have disk encryption enabled  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 custom data at rest.  Monitored via 5 checks	onmental Security Procedure
Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.  Monitored via 3 checks  Staff devices should have disk encryption enabled  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 custom data at rest.  Monitored via 5 checks	it Procedure
Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.  Monitored via 3 checks  Staff devices should have disk encryption enabled  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 custon data at rest.  Monitored via 5 checks	Policy
encrypted to protect from unauthorized access.  Monitored via 3 checks  Staff devices should have disk encryption enabled  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 custom data at rest.  Monitored via 5 checks	
Staff devices should have disk encryption enabled  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 custom data at rest.  Monitored via 5 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 custom data at rest.  Monitored via 5 checks	cks
Endpoint Security Policy  Control SDC 49  Entity has set up cryptographic mechanisms to encrypt all production database[s] that store custom data at rest.  Monitored via 5 checks	Id have disk encryption enabled
Control SDC 49  Entity has set up cryptographic mechanisms to encrypt all production database[s] that store custom data at rest.  Monitored via 5 checks	ld have disk encryption enabled
Entity has set up cryptographic mechanisms to encrypt all production database[s] that store custon data at rest.  Monitored via 5 checks	Policy
data at rest.  Monitored via 5 checks	
	ryptographic mechanisms to encrypt all production database[s] that store customer
Data at rest should be encrypted	:ks
	I be encrypted
Data at rest should be encrypted	I be encrypted
Encryption Policy	<b>✓</b>

# Asset 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 1 check Production systems should be secured with HTTPS 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

# 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

Critical Infrastructure assets should be identified



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	<b>✓</b>
Endpoint Security Policy	<b>✓</b>
Asset Management Policy	<b>✓</b>
Physical and Environmental Security Procedure	<b>✓</b>
Asset Management Procedure	<b>✓</b>

# 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

<b>✓</b>
<b>✓</b>
<b>✓</b>
<b>✓</b>

# CC7

# **System Operations**

# CC7.1

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

# 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	<b>✓</b>
Health of production infrastructure should be monitored	<b>✓</b>
Operation Security Policy	<b>✓</b>
Operations Security Procedure	<b>✓</b>



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

# Monitored via 2 checks





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

# Monitored via 2 checks





**SDC 55** 

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

# Monitored via 1 check

Vulnerability Scanning & Resolution Report





**SDC 56** 

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

#### Monitored via 1 check

Vulnerability Scanning & Resolution Report



# 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



**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.

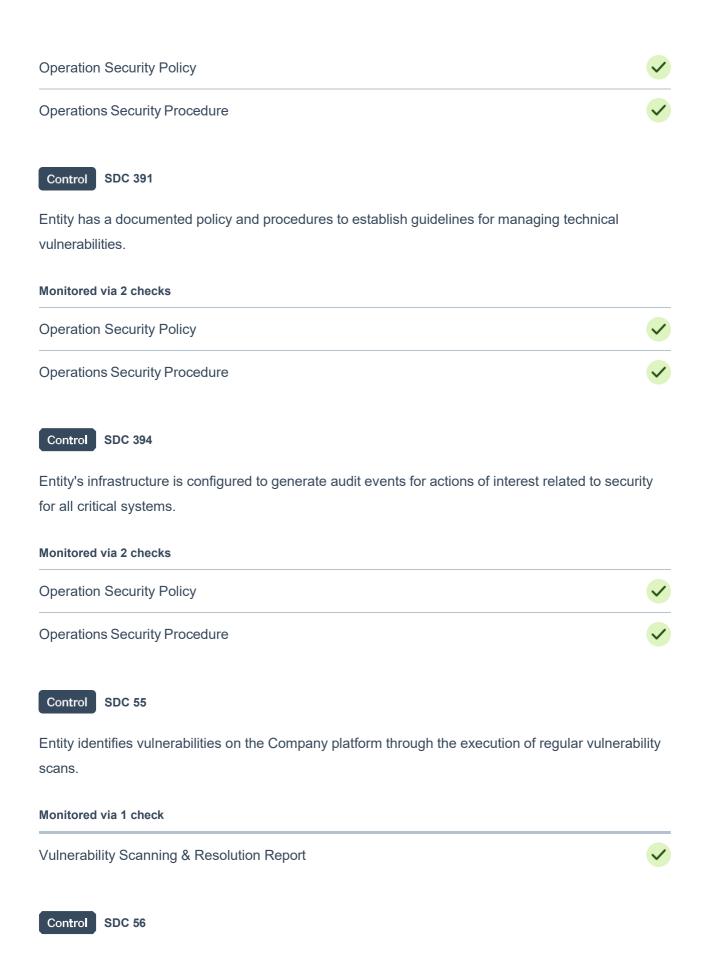
#### Monitored via 4 checks

Health of production infrastructure should be monitored



Health of production infrastructure should be monitored





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

#### Monitored via 1 check

Vulnerability Scanning & Resolution Report



# 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



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

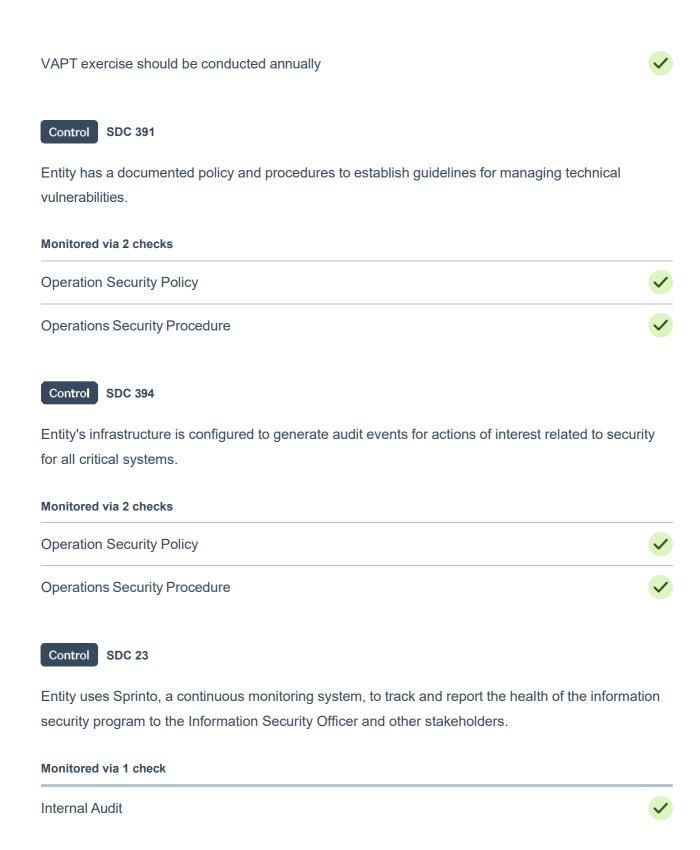
>
>
>
> Health of production infrastructure should be monitored Health of production infrastructure should be monitored **Operation Security Policy Operations Security Procedure** 



**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



# 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





**SDC 55** 

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

# Monitored via 1 check

Vulnerability Scanning & Resolution Report



# 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 Scanning & Resolution Report



# Control

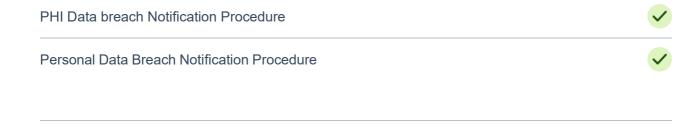
**SDC 112** 

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

# Monitored via 3 checks

**Data Breach Notification Policy** 





# **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



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.



Entity has established a policy and procedure which includes guidelines to be undertaken in response



# CC7.5

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

# 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 **SDC 393** Control 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

# **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



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

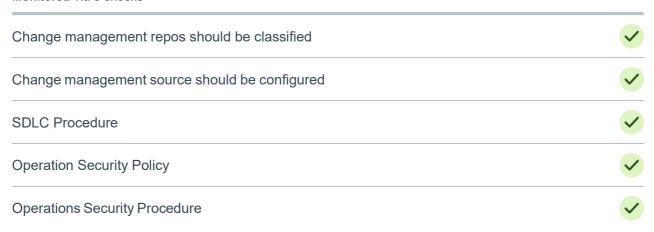
# Monitored via 4 checks





Entity has procedures to govern changes to its operating environment.

# Monitored via 5 checks



Control SDC 66

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

# Monitored via 5 checks





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

# 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



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



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 1 check

Vendor Management Policy



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.

Control SDC 6

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

# Monitored via 2 checks

Policies should be acknowledged by onboarded staff

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

Policies should be acknowledged by onboarded staff

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 3 checks

Staff devices should have disk encryption enabled

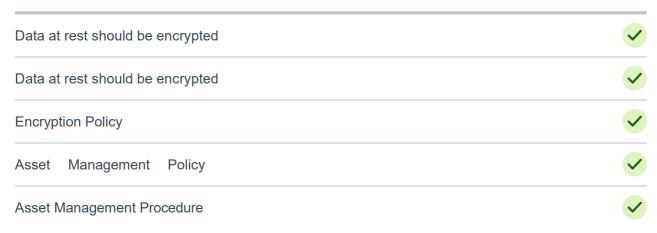
Staff devices should have disk encryption enabled

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 5 checks





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

# Monitored via 1 check

Information Security Policy



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.



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