

Vanta

<

Home

Tests

DOCUMENT

Documents

Policies

Risk assessment

REPORT

Compliance

Trust Report

MANAGE

People

Groups

Computers

Checklists

Access

Inventory

Vulnerabilities

Vendors

Integrations

Get started

Help

nexus.net

SOC 2

Edit system description

+ Add custom c

Controls

21%

17 completed80 total

Tests16/4933%

Documents1/422%

Audit timeline

No audit scheduled. Contact your auditor to ent

NowNovJanMarMa

Search controls

Filter by

Status

Owner

Jump to section

CC 1.1

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

	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Code of Conduct acknowledged b...	0/2	Administrative	Unassigned	CC 1.1
<input type="checkbox"/>	Confidentiality Agreement acknow...	0/2	Administrative	Unassigned	CC 1.1
<input type="checkbox"/>	Confidentiality Agreement acknow...	0/3	Administrative	Unassigned	CC 1.1
<input type="checkbox"/>	Employee background checks perf...	0/3	Administrative	Unassigned	CC 1.1 · CC 1.4
<input type="checkbox"/>	Performance evaluations conducted	0/1	Administrative	Unassigned	CC 1.1 · CC 1.4 · C
<input type="checkbox"/>	Code of Conduct acknowledged b...	0/2	Administrative	Unassigned	CC 1.1 · CC 1.5

CC 1.2

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

	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Board expertise developed	0/2	Administrative	Unassigned	CC 1.2
<input type="checkbox"/>	Board meetings conducted	0/1	Administrative	Unassigned	CC 1.2
<input type="checkbox"/>	Board oversight briefings conducted	0/1	Administrative	Unassigned	CC 1.2
<input type="checkbox"/>	Board charter documented	0/1	Administrative	Unassigned	CC 1.2 · CC 1.3

CC 1.3

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

--	--	--	--	--	--

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Board charter documented	0/1	Administrative	Unassigned	CC 1.2 · CC 1.3
<input type="checkbox"/>	Organization structure documented	0/1	Administrative	Unassigned	CC 1.3
<input type="checkbox"/>	Roles and responsibilities specified	0/2	Administrative	Unassigned	CC 1.3 · CC 1.4 · CC 1.5
<input type="checkbox"/>	Management roles and responsibilities documented	0/2	Administrative	Unassigned	CC 1.3 · CC 2.2

CC 1.4

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with the organization's strategy, objectives, and risks.

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Employee background checks performed	0/3	Administrative	Unassigned	CC 1.1 · CC 1.4
<input type="checkbox"/>	Performance evaluations conducted	0/1	Administrative	Unassigned	CC 1.1 · CC 1.4 · CC 1.5
<input type="checkbox"/>	Roles and responsibilities specified	0/2	Administrative	Unassigned	CC 1.3 · CC 1.4 · CC 1.5
<input type="checkbox"/>	Security awareness training implemented	1/4	Administrative	Unassigned	CC 1.4 · CC 2.2

CC 1.5

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Performance evaluations conducted	0/1	Administrative	Unassigned	CC 1.1 · CC 1.4 · CC 1.5
<input type="checkbox"/>	Code of Conduct acknowledged by employees	0/2	Administrative	Unassigned	CC 1.1 · CC 1.5
<input type="checkbox"/>	Roles and responsibilities specified	0/2	Administrative	Unassigned	CC 1.3 · CC 1.4 · CC 1.5

CC 2.1

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Control self-assessments conducted	1/1	Administrative	Unassigned	CC 2.1 · CC 4.1 · CC 4.2
<input type="checkbox"/>	Vulnerabilities scanned and remediated	0/3	Technical	Unassigned	CC 2.1 · CC 4.1 · CC 4.2
<input type="checkbox"/>	Log management utilized	1/3	Technical	Unassigned	CC 2.1 · CC 7.2

CC 2.2

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Roles and responsibilities specified	<div><div></div></div> 0/2	Administrative	Unassigned	CC 1.3 · CC 1.4 · CC 2.2
<input type="checkbox"/>	Management roles and responsibilities	<div><div></div></div> 0/2	Administrative	Unassigned	CC 1.3 · CC 2.2
<input type="checkbox"/>	Security awareness training implemented	<div><div></div></div> 1/4	Administrative	Unassigned	CC 1.4 · CC 2.2
<input type="checkbox"/>	System changes communicated	<div><div></div></div> 0/1	Administrative	Unassigned	CC 2.2
<input type="checkbox"/>	Whistleblower policy established	<div><div></div></div> 0/2	Administrative	Unassigned	CC 2.2
<input type="checkbox"/>	Service description communicated	<div><div></div></div> 0/2	Administrative	Unassigned	CC 2.2 · CC 2.3
<input type="checkbox"/>	Security policies established and reviewed	<div><div></div></div> 2/17	Administrative	Unassigned	CC 2.2 · CC 5.1 · CC 5.3
<input type="checkbox"/>	Incident response policies established	<div><div></div></div> 0/1	Administrative	Unassigned	CC 2.2 · CC 5.3 · CC 5.4

CC 2.3

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Service description communicated	<div><div></div></div> 0/2	Administrative	Unassigned	CC 2.2 · CC 2.3
<input type="checkbox"/>	Company commitments externally communicated	<div><div></div></div> 0/3	Administrative	Unassigned	CC 2.3
<input type="checkbox"/>	External support resources available	<div><div></div></div> 0/2	Administrative	Unassigned	CC 2.3
<input type="checkbox"/>	Support system available	<div><div></div></div> 0/3	Technical	Unassigned	CC 2.3
<input type="checkbox"/>	System changes externally communicated	<div><div></div></div> 0/4	Administrative	Unassigned	CC 2.3
<input type="checkbox"/>	Third-party agreements established	<div><div></div></div> 0/4	Administrative	Unassigned	CC 2.3 · CC 9.2

CC 3.1

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Risk management program established	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.1 · CC 3.2 · CC 3.3
<input type="checkbox"/>	Risk assessment objectives specified	<div><div></div></div> 0/2	Administrative	Unassigned	CC 3.1 · CC 5.3

CC 3.2

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Risk management program established	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.1 · CC 3.2 · CC 3.3
<input type="checkbox"/>	Risks assessments performed	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.2 · CC 3.3 · CC 3.4
<input type="checkbox"/>	Vendor management program established	<div><div></div></div> 0/3	Administrative	Unassigned	CC 3.2 · CC 4.1 · CC 4.2
<input type="checkbox"/>	Continuity and disaster recovery plan	<div><div></div></div> 0/2	Administrative	Unassigned	CC 3.2 · CC 7.5

CC 3.3

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Risk management program established	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.1 · CC 3.2 · CC 3.3
<input type="checkbox"/>	Risks assessments performed	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.2 · CC 3.3 · CC 3.4

CC 3.4

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Risk management program established	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.1 · CC 3.2 · CC 3.3
<input type="checkbox"/>	Risks assessments performed	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.2 · CC 3.3 · CC 3.4
<input type="checkbox"/>	Penetration testing performed	<div><div></div></div> 0/4	Technical	Unassigned	CC 3.4 · CC 4.1 · CC 4.2
<input type="checkbox"/>	Configuration management system	<div><div></div></div> 0/2	Technical	Unassigned	CC 3.4 · CC 7.1

CC 4.1

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Control self-assessments conducted	<div><div></div></div> 1/1	Administrative	Unassigned	CC 2.1 · CC 4.1 · CC 4.2
<input type="checkbox"/>	Vulnerabilities scanned and remediated	<div><div></div></div> 0/3	Technical	Unassigned	CC 2.1 · CC 4.1 · CC 4.2
<input type="checkbox"/>	Vendor management program established	<div><div></div></div> 0/3	Administrative	Unassigned	CC 3.2 · CC 4.1 · CC 4.2
<input type="checkbox"/>	Penetration testing performed	<div><div></div></div> 0/4	Technical	Unassigned	CC 3.4 · CC 4.1 · CC 4.2

CC 4.2

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Control self-assessments conduct...	<div><div></div>1/1</div>	Administrative	Unassigned	CC 2.1 · CC 4.1 · C
<input type="checkbox"/>	Vendor management program esta...	<div><div></div>0/3</div>	Administrative	Unassigned	CC 3.2 · CC 4.1 ·

CC 5.1

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Security policies established and r...	<div><div></div>2/17</div>	Administrative	Unassigned	CC 2.2 · CC 5.1 ·
<input type="checkbox"/>	Risk management program establi...	<div><div></div>0/1</div>	Administrative	Unassigned	CC 3.1 · CC 3.2 ·

CC 5.2






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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Security policies established and r...	<div><div></div>2/17</div>	Administrative	Unassigned	CC 2.2 · CC 5.1 ·
<input type="checkbox"/>	Development lifecycle established	<div><div></div>0/1</div>	Administrative	Unassigned	CC 5.2 · CC 5.3 ·
<input type="checkbox"/>	Access control procedures establi...	<div><div></div>1/4</div>	Administrative	Unassigned	CC 5.2 · CC 6.1 ·

CC 5.3



















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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Roles and responsibilities specified	<div><div></div>0/2</div>	Administrative	Unassigned	CC 1.3 · CC 1.4 ·
<input type="checkbox"/>	Security policies established and r...	<div><div></div>2/17</div>	Administrative	Unassigned	CC 2.2 · CC 5.1 ·
<input type="checkbox"/>	Incident response policies establis...	<div><div></div>0/1</div>	Administrative	Unassigned	CC 2.2 · CC 5.3 ·
<input type="checkbox"/>	Risk management program establi...	<div><div></div>0/1</div>	Administrative	Unassigned	CC 3.1 · CC 3.2 ·
<input type="checkbox"/>	Risk assessment objectives specifi...	<div><div></div>0/2</div>	Administrative	Unassigned	CC 3.1 · CC 5.3

<input type="checkbox"/>	Vendor management program esta...	 0/3	Administrative	Unassigned	CC 3.2 · CC 4.1 ·
<input type="checkbox"/>	Development lifecycle established	 0/1	Administrative	Unassigned	CC 5.2 · CC 5.3 ·
<input type="checkbox"/>	Backup processes established	 0/3	Administrative	Unassigned	CC 5.3
<input type="checkbox"/>	Data retention procedures establis...	 0/1	Administrative	Unassigned	CC 5.3 · CC 6.5
<input type="checkbox"/>	Change management procedures ...	 0/2	Technical	Unassigned	CC 5.3 · CC 7.1 ·

**CC 6.1**

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Access control procedures establi...	 1/4	Administrative	Unassigned	CC 5.2 · CC 6.1 ·
<input type="checkbox"/>	Data classification policy establish...	 0/1	Administrative	Unassigned	CC 6.1
<input type="checkbox"/>	Data encryption utilized	 0/0	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Encryption key access restricted	 0/1	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Firewall access restricted	 2/2	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Network segmentation implemented	 0/1	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Password policy enforced	 1/1	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Production application access rest...	 1/1	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Production database access restri...	 0/0	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Production inventory maintained	 0/3	Administrative	Unassigned	CC 6.1
<input type="checkbox"/>	Production network access restric...	 0/0	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Production OS access restricted	 1/1	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Unique account authentication enf...	 1/1	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Unique production database authen...	 0/0	Technical	Unassigned	CC 6.1
<input type="checkbox"/>	Access requests required	 1/2	Administrative	Unassigned	CC 6.1 · CC 6.2 ·
<input type="checkbox"/>	Unique network system authentica...	 0/0	Technical	Unassigned	CC 6.1 · CC 6.2 ·
<input type="checkbox"/>	Remote access encrypted enforced	 0/0	Technical	Unassigned	CC 6.1 · CC 6.6
<input type="checkbox"/>	Remote access MFA enforced	 0/1	Technical	Unassigned	CC 6.1 · CC 6.6

SOC 2 - Vanta

Production deployment access res...

0/2

Technical

Unassigned

CC 6.1 · CC 8.1

CC 6.2

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

	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
	Access control procedures establi...	1/4	Administrative	Unassigned	CC 5.2 · CC 6.1 ·
	Access requests required	1/2	Administrative	Unassigned	CC 6.1 · CC 6.2 ·
	Unique network system authentica...	0/0	Technical	Unassigned	CC 6.1 · CC 6.2 ·
	Access reviews conducted	3/4	Administrative	Unassigned	CC 6.2 · CC 6.3 ·
	Access revoked upon termination	1/3	Administrative	Unassigned	CC 6.2 · CC 6.3 ·

CC 6.3

The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of the entity's objectives.

	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
	Access control procedures establi...	1/4	Administrative	Unassigned	CC 5.2 · CC 6.1 ·
	Access requests required	1/2	Administrative	Unassigned	CC 6.1 · CC 6.2 ·
	Unique network system authentica...	0/0	Technical	Unassigned	CC 6.1 · CC 6.2 ·
	Access reviews conducted	3/4	Administrative	Unassigned	CC 6.2 · CC 6.3 ·
	Access revoked upon termination	1/3	Administrative	Unassigned	CC 6.2 · CC 6.3 ·

CC 6.4

The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up and other sensitive locations) to authorized personnel to meet the entity's objectives.

	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
	Access reviews conducted	3/4	Administrative	Unassigned	CC 6.2 · CC 6.3 ·
	Data center access reviewed	0/1	Physical	Unassigned	CC 6.4
	Physical access processes establi...	0/1	Physical	Unassigned	CC 6.4

<input type="checkbox"/>	Visitor procedures enforced	<div><div></div></div> 0/1	Physical	Unassigned	CC 6.4
--------------------------	-----------------------------	----------------------------	----------	------------	--------

CC 6.5

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Data retention procedures establis...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 5.3 · CC 6.5
<input type="checkbox"/>	Access revoked upon termination	<div><div></div></div> 1/3	Administrative	Unassigned	CC 6.2 · CC 6.3 ·
<input type="checkbox"/>	Asset disposal procedures utilized	<div><div></div></div> 1/3	Administrative	Unassigned	CC 6.5
<input type="checkbox"/>	Customer data deleted upon leave	<div><div></div></div> 0/2	Technical	Unassigned	CC 6.5

CC 6.6

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Unique network system authentica...	<div><div></div></div> 0/0	Technical	Unassigned	CC 6.1 · CC 6.2 ·
<input type="checkbox"/>	Remote access encrypted enforced	<div><div></div></div> 0/0	Technical	Unassigned	CC 6.1 · CC 6.6
<input type="checkbox"/>	Remote access MFA enforced	<div><div></div></div> 0/1	Technical	Unassigned	CC 6.1 · CC 6.6
<input type="checkbox"/>	Network firewalls reviewed	<div><div></div></div> 1/1	Technical	Unassigned	CC 6.6
<input type="checkbox"/>	Network firewalls utilized	<div><div></div></div> 1/1	Technical	Unassigned	CC 6.6
<input type="checkbox"/>	Data transmission encrypted	<div><div></div></div> 4/5	Technical	Unassigned	CC 6.6 · CC 6.7
<input type="checkbox"/>	Service infrastructure maintained	<div><div></div></div> 0/2	Technical	Unassigned	CC 6.6 · CC 6.8 ·
<input type="checkbox"/>	Intrusion detection system utilized	<div><div></div></div> 0/3	Technical	Unassigned	CC 6.6 · CC 7.2
<input type="checkbox"/>	Network and system hardening st...	<div><div></div></div> 1/1	Administrative	Unassigned	CC 6.6 · CC 8.1

CC 6.7

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Data transmission encrypted	<div><div></div></div> 4/5	Technical	Unassigned	CC 6.6 · CC 6.7
<input type="checkbox"/>	MDM system utilized	<div><div></div></div> 1/1	Technical	Unassigned	CC 6.7



<input type="checkbox"/>	Portable media encrypted	<div><div></div></div> 0/3	Technical	Unassigned	CC 6.7
--------------------------	--------------------------	----------------------------	-----------	------------	--------

CC 6.8

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Development lifecycle established	<div><div></div></div> 0/1	Administrative	Unassigned	CC 5.2 · CC 5.3 ·
<input type="checkbox"/>	Service infrastructure maintained	<div><div></div></div> 0/2	Technical	Unassigned	CC 6.6 · CC 6.8 ·
<input type="checkbox"/>	Anti-malware technology utilized	<div><div></div></div> 1/2	Technical	Unassigned	CC 6.8

CC 7.1

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Vulnerabilities scanned and remed...	<div><div></div></div> 0/3	Technical	Unassigned	CC 2.1 · CC 4.1 · C
<input type="checkbox"/>	Risks assessments performed	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.2 · CC 3.3 ·
<input type="checkbox"/>	Configuration management syste...	<div><div></div></div> 0/2	Technical	Unassigned	CC 3.4 · CC 7.1
<input type="checkbox"/>	Change management procedures ...	<div><div></div></div> 0/2	Technical	Unassigned	CC 5.3 · CC 7.1 · C
<input type="checkbox"/>	Vulnerability and system monitorin...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 7.1 · CC 7.2

CC 7.2

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Vulnerabilities scanned and remed...	<div><div></div></div> 0/3	Technical	Unassigned	CC 2.1 · CC 4.1 · C
<input type="checkbox"/>	Log management utilized	<div><div></div></div> 1/3	Technical	Unassigned	CC 2.1 · CC 7.2
<input type="checkbox"/>	Penetration testing performed	<div><div></div></div> 0/4	Technical	Unassigned	CC 3.4 · CC 4.1 ·
<input type="checkbox"/>	Service infrastructure maintained	<div><div></div></div> 0/2	Technical	Unassigned	CC 6.6 · CC 6.8 ·
<input type="checkbox"/>	Intrusion detection system utilized	<div><div></div></div> 0/3	Technical	Unassigned	CC 6.6 · CC 7.2
<input type="checkbox"/>	Vulnerability and system monitorin...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 7.1 · CC 7.2

<input type="checkbox"/>	Infrastructure performance monito...	<div><div></div></div> 1/5	Technical	Unassigned	CC 7.2
--------------------------	--------------------------------------	----------------------------	-----------	------------	--------

CC 7.3

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Incident response policies establis...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 2.2 · CC 5.3 ·
<input type="checkbox"/>	Incident management procedures ...	<div><div></div></div> 0/2	Administrative	Unassigned	CC 7.3 · CC 7.4 ·

CC 7.4

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Vulnerabilities scanned and remed...	<div><div></div></div> 0/3	Technical	Unassigned	CC 2.1 · CC 4.1 · CC 7.4 ·
<input type="checkbox"/>	Incident response policies establis...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 2.2 · CC 5.3 ·
<input type="checkbox"/>	Service infrastructure maintained	<div><div></div></div> 0/2	Technical	Unassigned	CC 6.6 · CC 6.8 ·
<input type="checkbox"/>	Incident management procedures ...	<div><div></div></div> 0/2	Administrative	Unassigned	CC 7.3 · CC 7.4 ·
<input type="checkbox"/>	Incident response plan tested	<div><div></div></div> 0/3	Administrative	Unassigned	CC 7.4 · CC 7.5

CC 7.5

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Incident response policies establis...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 2.2 · CC 5.3 ·
<input type="checkbox"/>	Continuity and disaster recovery p...	<div><div></div></div> 0/2	Administrative	Unassigned	CC 3.2 · CC 7.5
<input type="checkbox"/>	Incident management procedures ...	<div><div></div></div> 0/2	Administrative	Unassigned	CC 7.3 · CC 7.4 ·
<input type="checkbox"/>	Incident response plan tested	<div><div></div></div> 0/3	Administrative	Unassigned	CC 7.4 · CC 7.5

CC 8.1

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
--------------------------	---------	-----------------	----------	-------	---------------

## SOC 2 - Vanta

<input type="checkbox"/>	Vulnerabilities scanned and remediated	<div><div></div></div> 0/3	Technical	Unassigned	CC 2.1 · CC 4.1 · CC 5.1
<input type="checkbox"/>	Penetration testing performed	<div><div></div></div> 0/4	Technical	Unassigned	CC 3.4 · CC 4.1 · CC 5.1
<input type="checkbox"/>	Development lifecycle established	<div><div></div></div> 0/1	Administrative	Unassigned	CC 5.2 · CC 5.3 · CC 5.4
<input type="checkbox"/>	Change management procedures established	<div><div></div></div> 0/2	Technical	Unassigned	CC 5.3 · CC 7.1 · CC 7.2
<input type="checkbox"/>	Production deployment access restricted	<div><div></div></div> 0/2	Technical	Unassigned	CC 6.1 · CC 8.1
<input type="checkbox"/>	Service infrastructure maintained	<div><div></div></div> 0/2	Technical	Unassigned	CC 6.6 · CC 6.8 · CC 8.1
<input type="checkbox"/>	Network and system hardening standards established	<div><div></div></div> 1/1	Administrative	Unassigned	CC 6.6 · CC 8.1

## CC 9.1

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Risk management program establi...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.1 · CC 3.2 ·
<input type="checkbox"/>	Risks assessments performed	<div><div></div></div> 0/1	Administrative	Unassigned	CC 3.2 · CC 3.3 ·
<input type="checkbox"/>	Continuity and Disaster Recovery ...	<div><div></div></div> 0/1	Administrative	Unassigned	CC 9.1
<input type="checkbox"/>	Cybersecurity insurance maintained	<div><div></div></div> 0/1	Administrative	Unassigned	CC 9.1

## CC 9.2

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

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	Third-party agreements established	<div><div></div></div> 0/4	Administrative	Unassigned	CC 2.3 · CC 9.2
<input type="checkbox"/>	Vendor management program esta...	<div><div></div></div> 0/3	Administrative	Unassigned	CC 3.2 · CC 4.1 ·

## SD - SOC 2

Description of the organization's system and commitments for Section III of the audit report

<input type="checkbox"/>	CONTROL	EVIDENCE STATUS	CATEGORY	OWNER	STANDARD CODE
<input type="checkbox"/>	SOC 2 - System Description	<span>1/1</span>	Administrative	Unassigned	SD - SOC 2