

SOC 2 Gap Assessment from Vanta

FOR SHUTTLEROCK

The American Institute of Certified Public Accountants (AICPA) defined the SOC (System and Organization Controls) reporting framework to help businesses manage risks. Their SOC 2 standard defines criteria for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality, and privacy.

Vanta performed a gap analysis of Shutterstock's security and IT infrastructure in preparation for a SOC 2 audit. Vanta's SOC 2 analysis identified gaps in Shutterstock's infrastructure and provided steps to correct them.

In this report, Vanta:

- Tests a complete set of security and infrastructure controls that may appear in a SOC 2 audit
- Identifies gaps and vulnerabilities in infrastructure and processes

Intended use

This gap assessment can be used by:

- Shutterstock to identify issues critical for remediation
- Shutterstock's customers to understand the company's progress toward SOC 2 compliance

Continuous gap assessment approach: continuous monitoring

Vanta continuously monitors the company's policies, procedures, and IT infrastructure to ensure the company adheres to AICPA's Trust Service Principles of security, availability, and confidentiality.

To do this, Vanta connects directly to the company's infrastructure accounts, version control tools, task trackers, endpoints, hosts, HR tools, and internal policies. Vanta then continuously monitors these resources to determine if Shutterstock meets the SOC 2 standard.

In compiling this gap assessment, Vanta took into account Shutterstock's unique requirements and technical environment, including business model, products and services, and interactions with customer data.

Control Environment

CC 1.1

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

5 CONTROLS

► Code of Conduct acknowledged by contractors ✓ COMPLETE

The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.

2 TESTS

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to the Code of Conduct. ✓

Company has a Code of Conduct: Verifies that the Code of Conduct is in place and has been approved within Vanta. ✓

1 DOCUMENT

Contractor agreement ✓

► Code of Conduct acknowledged by employees and enforced ✓ COMPLETE

The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.

4 TESTS

Employees agree to Acceptable Use Policy: Verifies that all relevant employees have agreed to the Acceptable Use Policy. ✓

Company has an Acceptable Use Policy: Verifies that the Acceptable Use Policy is in place and has been approved within Vanta. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to the Code of Conduct. ✓

Company has a Code of Conduct: Verifies that the Code of Conduct is in place and has been approved within Vanta. ✓

- Confidentiality Agreement acknowledged by contractors ✓ COMPLETE
- The company requires contractors to sign a confidentiality agreement at the time of engagement.
- 1 DOCUMENT
- Contractor agreement** ✓
-
- Confidentiality Agreement acknowledged by employees ✓ COMPLETE
- The company requires employees to sign a confidentiality agreement during onboarding.
- 2 DOCUMENTS
- Employee agreement** ✓
- Signed confidentiality agreement** ✓
-
- Employee background checks performed ✓ COMPLETE
- The company performs background checks on new employees.
- 1 TEST
- Background checks on new hires:** Verifies that all employees for whom a background check is required have a background check on file. ✓
- 1 DOCUMENT
- Completed employee background checks** ✓
-

CC 1.2

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

- 4 CONTROLS
- Board charter documented ✓ COMPLETE
- The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
- 1 DOCUMENT
- Board of directors charter** ✓
-

► Board expertise developed ✓ COMPLETE

The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.

2 DOCUMENTS

Board of directors CVs ✓

Board of directors charter ✓

► Board meetings conducted ✓ COMPLETE

The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.

1 DOCUMENT

Board of directors meeting minutes and agenda ✓

► Board oversight briefings conducted ✓ COMPLETE

The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.

1 DOCUMENT

Board of directors meeting minutes and agenda ✓

CC 1.3

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

4 CONTROLS

► Board charter documented ✓ COMPLETE

The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.

1 DOCUMENT

Board of directors charter ✓

► Management roles and responsibilities defined ✓ COMPLETE

The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

1 TEST

Security Officer Role assigned and communicated: Verifies that the Information Security Policy is in place and has been approved within Vanta.



► Organization structure documented ✓ COMPLETE

The company maintains an organizational chart that describes the organizational structure and reporting lines.

1 DOCUMENT

Company organization chart



► Roles and responsibilities specified ✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles



CC 1.4

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

3 CONTROLS

► Employee background checks performed ✓ COMPLETE

The company performs background checks on new employees.

1 TEST

Background checks on new hires: Verifies that all employees for whom a background check is required have a background check on file.



1 DOCUMENT

Completed employee background checks



► Roles and responsibilities specified ✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles ✓

► Security awareness training implemented ✓ COMPLETE

The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

2 TESTS

Policies for security awareness training: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy requires security awareness training. ✓

Security awareness training selected: Verifies that a security awareness training program has been selected within Vanta. ✓

1 DOCUMENT

Security awareness training completion ✓

CC 1.5

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

2 CONTROLS

► Code of Conduct acknowledged by employees and enforced ✓ COMPLETE

The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.

4 TESTS

Employees agree to Acceptable Use Policy: Verifies that all relevant employees have agreed to the Acceptable Use Policy. ✓

Company has an Acceptable Use Policy: Verifies that the Acceptable Use Policy is in place and has been approved within Vanta. ✓

Employees agree to Code of Conduct: Verifies that all relevant employees have agreed to the Code of Conduct. ✓

Company has a Code of Conduct: Verifies that the Code of Conduct is in place and has been approved within Vanta. ✓

► Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles



Communication and Information

CC 2.1

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

3 CONTROLS

▶ Control self-assessments conducted

✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes.

✓

▶ Log management utilized

✓ COMPLETE

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.

6 TESTS

Heroku logs archived for 365 days: Verifies that all Heroku apps are using a plugin that stores logs for 365 days, or are using a custom log drain.

✓

User activity and API use is tracked (Heroku): This feature is built into Heroku.

✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta.

✓

Only authorized users can access logging buckets: Verifies that no AWS S3 logging buckets grant access to the built-in AWS groups AllUsers or AuthenticatedUsers

✓

S3 server access logs enabled: Verifies there is at least one AWS S3 bucket acting as a destination for server access logging or CloudTrail data event logging.

✓

Server logs retained for 365 days (AWS): Verifies that all AWS CloudWatch Log Groups are configured to retain logs for at least 365 days.

✓

▼ Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

CC 2.2

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

8 CONTROLS

► Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

Company Incident Response Plan cites responsible team members: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan names specific team members who are responsible for monitoring and responding to incidents. ✓

► Management roles and responsibilities defined ✓ COMPLETE

The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

1 TEST

Security Officer Role assigned and communicated: Verifies that the Information Security Policy is in place and has been approved within Vanta. ✓

► Roles and responsibilities specified ✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles ✓

► Security awareness training implemented ✓ COMPLETE

The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

2 TESTS

Policies for security awareness training: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy requires security awareness training. ✓

Security awareness training selected: Verifies that a security awareness training program has been selected within Vanta. ✓

1 DOCUMENT

Security awareness training completion ✓

► Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

39 TESTS

Company has a Business Continuity Plan: Verifies that the Business Continuity Plan is in place and has been approved within Vanta. ✓

Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta. ✓

Company has a Code of Conduct: Verifies that the Code of Conduct is in place and has been approved within Vanta. ✓

Security policies cover encryption: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Policies cover employee confidentiality regarding user data: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Policies cover employee access to user data: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Backup Policy: Verifies that the Backup Policy is in place and has been approved within Vanta. ✓

Company has a Data Classification Policy: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Company has a Data Protection Policy: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Disaster Recovery Plan: Verifies that the Disaster Recovery Plan is in place and has been approved within Vanta. ✓

Process for responsible disclosure by employees: Verifies that the Responsible Disclosure Policy and Acceptable Use Policy is in place and has been approved within Vanta. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Backup Policy: Verifies that all relevant employees have agreed to the Backup Policy. ✓

Employees agree to Business Continuity Plan: Verifies that all relevant employees have agreed to the Business Continuity Plan. ✓

Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy. ✓

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy. ✓

Employees agree to Data Classification Policy: Verifies that all relevant employees have agreed to the Data Classification Policy. ✓

Employees agree to Data Deletion Policy: Verifies that all relevant employees have agreed to the Data Deletion Policy. ✓

Employees agree to Data Protection Policy: Verifies that all relevant employees have agreed to the Data Protection Policy. ✓

Employees agree to Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Disaster Recovery Plan.	✓
Employees agree to Information Security Policy: Verifies that all relevant employees have agreed to the Information Security Policy.	✓
Employees agree to Password Policy: Verifies that all relevant employees have agreed to the Password Policy.	✓
Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy.	✓
Employees agree to Responsible Disclosure Policy: Verifies that all relevant employees have agreed to the Responsible Disclosure Policy.	✓
Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.	✓
Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy.	✓
Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy.	✓
Internal Password Policy for employee accounts: Verifies that the Password Policy is in place and has been approved within Vanta.	✓
Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.	✓
Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta.	✓
Company has a Responsible Disclosure Policy: Verifies that the Responsible Disclosure Policy is in place and has been approved within Vanta.	✓
Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.	✓
Company has a Data Deletion Policy: Verifies that the Data Deletion Policy is in place and has been approved within Vanta.	✓
Security team has a line of communication to the CEO: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy states that the security team has a line of communication to the CEO.	✓
Policies for a security team: Verifies that the Information Security Policy is in place and has been approved within Vanta.	✓
Policies for security awareness training: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy requires security awareness training.	✓
SLA for security bugs: Verifies that management has approved the Change Management Policy and that they have set an SLA on P0 security issues within Vanta.	✓
Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta.	✓

▶ Service description communicated ✓ COMPLETE

The company provides a description of its products and services to internal and external users.

2 DOCUMENTS

Network diagram ✓

Product documentation site ✓

▶ System changes communicated ✓ COMPLETE

The company communicates system changes to authorized internal users.

1 DOCUMENT

Internal communication for system updates ✓

▼ Whistleblower policy established ✓ COMPLETE

The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.

1 DOCUMENT

Anonymous whistleblower channel ✓

CC 2.3

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

6 CONTROLS

▶ Company commitments externally communicated ✓ COMPLETE

The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).

3 DOCUMENTS

MSA template ✓

Security information page ✓

Publicly available terms of service ✓

► External support resources available ✓ COMPLETE

The company provides guidelines and technical support resources relating to system operations to customers.

2 DOCUMENTS

Customer support site or email alias ✓

Public change log or release notes ✓

► Service description communicated ✓ COMPLETE

The company provides a description of its products and services to internal and external users.

2 DOCUMENTS

Network diagram ✓

Product documentation site ✓

► Support system available ✓ COMPLETE

The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.

3 DOCUMENTS

Customer support site or email alias ✓

Product documentation site ✓

Public change log or release notes ✓

► System changes externally communicated ✓ COMPLETE

The company notifies customers of critical system changes that may affect their processing.

4 DOCUMENTS

Customer support site or email alias ✓

Product documentation site ✓

Public change log or release notes ✓

Application status page ✓

▶ Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

1 TEST

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list.



3 DOCUMENTS

Cloud provider service agreement



Publicly available privacy policy



Publicly available terms of service



Risk Assessment

CC 3.1

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

2 CONTROLS

- ▶ Risk assessment objectives specified ✓ COMPLETE

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months. ✓

- ▶ Risk management program established ✓ COMPLETE

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program. ✓

Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta. ✓

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 determining how the risks should be managed.

4 CONTROLS

► Continuity and disaster recovery plans tested ✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Risk management program established ✓ COMPLETE

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program. ✓

Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta. ✓

► Risks assessments performed ✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months. ✓

► Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

5 TESTS

Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy.

✓

Company has compliance security reports for critical vendors and reviews them annually: Verifies that all high risk vendors [Vendors](/vendors) have a completed security review in the past 12 months.

✓

Policy to collect sub-service organization compliance reports: Verifies that management has approved the Vendor Management Policy and that the policy states that compliance reports are collected from external vendors.

✓

Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta.

✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list.

✓

CC 3.3

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

2 CONTROLS

► Risk management program established

✓ COMPLETE

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.

✓

Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.

✓

► Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months.

✓

CC 3.4

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

4 CONTROLS

► Configuration management system established

✓ COMPLETE

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

1 DOCUMENT

CI/CD system in use

✓

► Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

1 TEST

Records of penetration testing: Verifies that a periodic penetration test has been conducted recently and that evidence of that test has been uploaded to Vanta.

✓

2 DOCUMENTS

Penetration test report

✓

Penetration test remediation

✓

► Risk management program established

✓ COMPLETE

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.

✓

Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.

✓

► Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months.

✓

Monitoring Activities

CC 4.1

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.

4 CONTROLS

▶ Control self-assessments conducted ✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes. ✓

▶ Penetration testing performed ✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

1 TEST

Records of penetration testing: Verifies that a periodic penetration test has been conducted recently and that evidence of that test has been uploaded to Vanta. ✓

2 DOCUMENTS

Penetration test report ✓

Penetration test remediation ✓

► Vendor management program established ✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

5 TESTS

Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy. ✓

Company has compliance security reports for critical vendors and reviews them annually: Verifies that all high risk vendors [Vendors](/vendors) have a completed security review in the past 12 months. ✓

Policy to collect sub-service organization compliance reports: Verifies that management has approved the Vendor Management Policy and that the policy states that compliance reports are collected from external vendors. ✓

Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

► Vulnerabilities scanned and remediated ✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

CC 4.2

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.

2 CONTROLS

► Control self-assessments conducted ✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes. ✓

► Vendor management program established ✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

5 TESTS

Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy. ✓

Company has compliance security reports for critical vendors and reviews them annually: Verifies that all high risk vendors [Vendors](/vendors) have a completed security review in the past 12 months. ✓

Policy to collect sub-service organization compliance reports: Verifies that management has approved the Vendor Management Policy and that the policy states that compliance reports are collected from external vendors. ✓

Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

Control Activities

CC 5.1

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.

2 CONTROLS

► Risk management program established ✓ COMPLETE

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program. ✓

Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta. ✓

► Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

39 TESTS

Company has a Business Continuity Plan: Verifies that the Business Continuity Plan is in place and has been approved within Vanta. ✓

Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta. ✓

Company has a Code of Conduct: Verifies that the Code of Conduct is in place and has been approved within Vanta. ✓

Security policies cover encryption: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Policies cover employee confidentiality regarding user data: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Policies cover employee access to user data: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Backup Policy: Verifies that the Backup Policy is in place and has been approved within Vanta. ✓

Company has a Data Classification Policy: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Company has a Data Protection Policy: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Disaster Recovery Plan: Verifies that the Disaster Recovery Plan is in place and has been approved within Vanta. ✓

Process for responsible disclosure by employees: Verifies that the Responsible Disclosure Policy and Acceptable Use Policy is in place and has been approved within Vanta. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Backup Policy: Verifies that all relevant employees have agreed to the Backup Policy. ✓

Employees agree to Business Continuity Plan: Verifies that all relevant employees have agreed to the Business Continuity Plan. ✓

Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy. ✓

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy. ✓

Employees agree to Data Classification Policy: Verifies that all relevant employees have agreed to the Data Classification Policy. ✓

Employees agree to Data Deletion Policy: Verifies that all relevant employees have agreed to the Data Deletion Policy. ✓

Employees agree to Data Protection Policy: Verifies that all relevant employees have agreed to the Data Protection Policy. ✓

Employees agree to Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Disaster Recovery Plan.	✓
Employees agree to Information Security Policy: Verifies that all relevant employees have agreed to the Information Security Policy.	✓
Employees agree to Password Policy: Verifies that all relevant employees have agreed to the Password Policy.	✓
Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy.	✓
Employees agree to Responsible Disclosure Policy: Verifies that all relevant employees have agreed to the Responsible Disclosure Policy.	✓
Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.	✓
Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy.	✓
Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy.	✓
Internal Password Policy for employee accounts: Verifies that the Password Policy is in place and has been approved within Vanta.	✓
Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.	✓
Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta.	✓
Company has a Responsible Disclosure Policy: Verifies that the Responsible Disclosure Policy is in place and has been approved within Vanta.	✓
Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.	✓
Company has a Data Deletion Policy: Verifies that the Data Deletion Policy is in place and has been approved within Vanta.	✓
Security team has a line of communication to the CEO: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy states that the security team has a line of communication to the CEO.	✓
Policies for a security team: Verifies that the Information Security Policy is in place and has been approved within Vanta.	✓
Policies for security awareness training: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy requires security awareness training.	✓
SLA for security bugs: Verifies that management has approved the Change Management Policy and that they have set an SLA on P0 security issues within Vanta.	✓
Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta.	✓

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

3 CONTROLS

► Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

2 TESTS

Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy.

✓

Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.

✓

1 DOCUMENT

Access request ticket and history

✓

► Development lifecycle established

✓ COMPLETE

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

2 TESTS

Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta.

✓

Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy.

✓

► Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

39 TESTS

Company has a Business Continuity Plan: Verifies that the Business Continuity Plan is in place and has been approved within Vanta. ✓

Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta. ✓

Company has a Code of Conduct: Verifies that the Code of Conduct is in place and has been approved within Vanta. ✓

Security policies cover encryption: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Policies cover employee confidentiality regarding user data: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Policies cover employee access to user data: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Backup Policy: Verifies that the Backup Policy is in place and has been approved within Vanta. ✓

Company has a Data Classification Policy: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Company has a Data Protection Policy: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Disaster Recovery Plan: Verifies that the Disaster Recovery Plan is in place and has been approved within Vanta. ✓

Process for responsible disclosure by employees: Verifies that the Responsible Disclosure Policy and Acceptable Use Policy is in place and has been approved within Vanta. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Backup Policy: Verifies that all relevant employees have agreed to the Backup Policy. ✓

Employees agree to Business Continuity Plan: Verifies that all relevant employees have agreed to the Business Continuity Plan. ✓

Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy. ✓

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy. ✓

Employees agree to Data Classification Policy: Verifies that all relevant employees have agreed to the Data Classification Policy. ✓

Employees agree to Data Deletion Policy: Verifies that all relevant employees have agreed to the Data Deletion Policy. ✓

Employees agree to Data Protection Policy: Verifies that all relevant employees have agreed to the Data Protection Policy. ✓

Employees agree to Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Disaster Recovery Plan.	✓
Employees agree to Information Security Policy: Verifies that all relevant employees have agreed to the Information Security Policy.	✓
Employees agree to Password Policy: Verifies that all relevant employees have agreed to the Password Policy.	✓
Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy.	✓
Employees agree to Responsible Disclosure Policy: Verifies that all relevant employees have agreed to the Responsible Disclosure Policy.	✓
Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.	✓
Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy.	✓
Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy.	✓
Internal Password Policy for employee accounts: Verifies that the Password Policy is in place and has been approved within Vanta.	✓
Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.	✓
Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta.	✓
Company has a Responsible Disclosure Policy: Verifies that the Responsible Disclosure Policy is in place and has been approved within Vanta.	✓
Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.	✓
Company has a Data Deletion Policy: Verifies that the Data Deletion Policy is in place and has been approved within Vanta.	✓
Security team has a line of communication to the CEO: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy states that the security team has a line of communication to the CEO.	✓
Policies for a security team: Verifies that the Information Security Policy is in place and has been approved within Vanta.	✓
Policies for security awareness training: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy requires security awareness training.	✓
SLA for security bugs: Verifies that management has approved the Change Management Policy and that they have set an SLA on P0 security issues within Vanta.	✓
Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta.	✓

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

10 CONTROLS

► Backup processes established ✓ COMPLETE

The company's data backup policy documents requirements for backup and recovery of customer data.

2 TESTS

Company has a Backup Policy: Verifies that the Backup Policy is in place and has been approved within Vanta. ✓

Employees agree to Backup Policy: Verifies that all relevant employees have agreed to the Backup Policy. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Change management procedures enforced ✓ COMPLETE

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

1 TEST

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories. ✓

1 DOCUMENT

CI/CD system in use ✓

► Data retention procedures established ✓ COMPLETE

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

4 TESTS

Company has a Data Protection Policy: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Employees agree to Data Deletion Policy: Verifies that all relevant employees have agreed to the Data Deletion Policy. ✓

Employees agree to Data Protection Policy: Verifies that all relevant employees have agreed to the Data Protection Policy. ✓

Company has a Data Deletion Policy: Verifies that the Data Deletion Policy is in place and has been approved within Vanta. ✓

► Development lifecycle established

✓ COMPLETE

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

2 TESTS

Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta.

✓

Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy.

✓

► Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan.

✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents.

✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents.

✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta.

✓

Company Incident Response Plan cites responsible team members: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan names specific team members who are responsible for monitoring and responding to incidents.

✓

► Risk assessment objectives specified

✓ COMPLETE

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months.

✓

► Risk management program established

✓ COMPLETE

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.



Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.



► Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles



► Security policies established and reviewed

✓ COMPLETE

The company's information security policies and procedures are documented and reviewed at least annually.

39 TESTS

Company has a Business Continuity Plan: Verifies that the Business Continuity Plan is in place and has been approved within Vanta. ✓

Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta. ✓

Company has a Code of Conduct: Verifies that the Code of Conduct is in place and has been approved within Vanta. ✓

Security policies cover encryption: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Policies cover employee confidentiality regarding user data: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Policies cover employee access to user data: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Backup Policy: Verifies that the Backup Policy is in place and has been approved within Vanta. ✓

Company has a Data Classification Policy: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Company has a Data Protection Policy: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Company has a Disaster Recovery Plan: Verifies that the Disaster Recovery Plan is in place and has been approved within Vanta. ✓

Process for responsible disclosure by employees: Verifies that the Responsible Disclosure Policy and Acceptable Use Policy is in place and has been approved within Vanta. ✓

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

Employees agree to Backup Policy: Verifies that all relevant employees have agreed to the Backup Policy. ✓

Employees agree to Business Continuity Plan: Verifies that all relevant employees have agreed to the Business Continuity Plan. ✓

Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy. ✓

Employees agree to Cryptography Policy: Verifies that all relevant employees have agreed to the Cryptography Policy. ✓

Employees agree to Data Classification Policy: Verifies that all relevant employees have agreed to the Data Classification Policy. ✓

Employees agree to Data Deletion Policy: Verifies that all relevant employees have agreed to the Data Deletion Policy. ✓

Employees agree to Data Protection Policy: Verifies that all relevant employees have agreed to the Data Protection Policy. ✓

Employees agree to Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Disaster Recovery Plan.	✓
Employees agree to Information Security Policy: Verifies that all relevant employees have agreed to the Information Security Policy.	✓
Employees agree to Password Policy: Verifies that all relevant employees have agreed to the Password Policy.	✓
Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy.	✓
Employees agree to Responsible Disclosure Policy: Verifies that all relevant employees have agreed to the Responsible Disclosure Policy.	✓
Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.	✓
Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy.	✓
Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy.	✓
Internal Password Policy for employee accounts: Verifies that the Password Policy is in place and has been approved within Vanta.	✓
Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.	✓
Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta.	✓
Company has a Responsible Disclosure Policy: Verifies that the Responsible Disclosure Policy is in place and has been approved within Vanta.	✓
Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.	✓
Company has a Data Deletion Policy: Verifies that the Data Deletion Policy is in place and has been approved within Vanta.	✓
Security team has a line of communication to the CEO: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy states that the security team has a line of communication to the CEO.	✓
Policies for a security team: Verifies that the Information Security Policy is in place and has been approved within Vanta.	✓
Policies for security awareness training: Verifies that management has approved the Information Security Policy and that they have confirmed in Vanta that the policy requires security awareness training.	✓
SLA for security bugs: Verifies that management has approved the Change Management Policy and that they have set an SLA on P0 security issues within Vanta.	✓
Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta.	✓

► Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

5 TESTS

Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy.



Company has compliance security reports for critical vendors and reviews them annually: Verifies that all high risk vendors [Vendors](/vendors) have a completed security review in the past 12 months.



Policy to collect sub-service organization compliance reports: Verifies that management has approved the Vendor Management Policy and that the policy states that compliance reports are collected from external vendors.



Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta.



Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list.



Logical and Physical Access Controls

CC 6.1

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.

19 CONTROLS

▶ Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

2 TESTS

Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy.

✓

Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.

✓

1 DOCUMENT

Access request ticket and history

✓

▶ Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA.

✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week.

✓

Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.

✓

1 DOCUMENT

Access request ticket and history

✓

► Data classification policy established ✓ COMPLETE

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

2 TESTS

Company has a Data Classification Policy: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Employees agree to Data Classification Policy: Verifies that all relevant employees have agreed to the Data Classification Policy. ✓

► Data encryption utilized ✓ COMPLETE

The company's datastores housing sensitive customer data are encrypted at rest.

3 TESTS

User data is encrypted at rest: Verifies that all Amazon RDS instances are encrypted. ✓

User data is encrypted at rest (Heroku): Verifies that Heroku databases are encrypted at rest. This feature is automatically provided by Heroku Postgres plans on the Standard tier or higher. ✓

User data in S3 is encrypted at rest (AWS): Verifies that all AWS S3 buckets marked as containing user data are encrypted. ✓

► Encryption key access restricted ✓ COMPLETE

The company restricts privileged access to encryption keys to authorized users with a business need.

2 TESTS

Security policies cover encryption: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

► Firewall access restricted

✓ COMPLETE

The company restricts privileged access to the firewall to authorized users with a business need.

9 TESTS

EC2 instance public ports restricted (AWS): Verifies that each EC2 instance's attached Security Groups expose at most ports 80 and 443 to the public internet for protocols other than ICMP. ✓

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied: Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Personal firewalls required: Verifies that management has approved the Asset Management Policy and that they have confirmed in Vanta that the policy requires use of a personal firewall. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

► Network segmentation implemented

✓ COMPLETE

The company's network is segmented to prevent unauthorized access to customer data.

1 DOCUMENT

Network segregation ✓

► Password policy enforced

✓ COMPLETE

The company requires passwords for in-scope system components to be configured according to the company's policy.

1 TEST

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

► Production application access restricted

✓ COMPLETE

The company restricts privileged access to the application to authorized users with a business need.

9 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached.

✓

Employees have unique email accounts: Verifies that every linked identity provider has more than one user.

✓

Employees have unique version control accounts: Verifies that every linked version control account has more than one user.

✓

Service accounts used: Verifies that every AWS account is assigned a role.

✓

Service accounts used (Heroku): This feature is built into Heroku.

✓

Root infrastructure account unused: Verifies that the AWS root account has not been used in the last 30 days.

✓

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days.

✓

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users.

✓

No user account has a policy attached directly (Heroku): This feature is built into Heroku.

✓

► Production database access restricted

✓ COMPLETE

The company restricts privileged access to databases to authorized users with a business need.

2 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA.

✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

✓

► Production deployment access restricted

✓ COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

2 TESTS

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories.

✓

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days.

✓

► Production inventory maintained ✓ COMPLETE

The company maintains a formal inventory of production system assets.

3 TESTS

Inventory items have descriptions: Verifies that all items on the Vanta inventory page have descriptions. ✓

Inventory items have owners: Verifies that all items on the Vanta inventory page have been assigned owners. ✓

Inventory list tracks resources that contain user data: Verifies that these resource types - storage buckets, databases, PaaS apps, queues, data warehouses, or custom items - are marked as containing user data in Vanta. ✓

► Production network access restricted ✓ COMPLETE

The company restricts privileged access to the production network to authorized users with a business need.

2 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

► Production OS access restricted ✓ COMPLETE

The company restricts privileged access to the operating system to authorized users with a business need.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

► Remote access encrypted enforced ✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

2 TESTS

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

► Remote access MFA enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

5 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

MFA on Google Workspace: Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled. ✓

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled. ✓

Company requires MFA where possible: Verifies that management has approved the Password Policy and that they have confirmed in Vanta that the plan requires multi-factor authentication on all accounts. ✓

► Unique account authentication enforced

✓ COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

10 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached. ✓

Employees have unique email accounts: Verifies that every linked identity provider has more than one user. ✓

Employees have unique version control accounts: Verifies that every linked version control account has more than one user. ✓

Service accounts used: Verifies that every AWS account is assigned a role. ✓

Service accounts used (Heroku): This feature is built into Heroku. ✓

Root infrastructure account unused: Verifies that the AWS root account has not been used in the last 30 days. ✓

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days. ✓

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users. ✓

No user account has a policy attached directly (Heroku): This feature is built into Heroku. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

► Unique network system authentication enforced ✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

4 TESTS

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

► Unique production database authentication enforced ✓ COMPLETE

The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.

5 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

MFA on Google Workspace: Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled. ✓

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled. ✓

CC 6.2

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.

5 CONTROLS

► Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

2 TESTS

Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy.



Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.



1 DOCUMENT

Access request ticket and history



► Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA.



GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week.



Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta.



1 DOCUMENT

Access request ticket and history



► Access reviews conducted

✓ COMPLETE

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

9 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

GitHub accounts associated with users: Verifies that all GitHub accounts have been linked to users within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that Google Workspace, Office 365, or Okta has been linked to Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Jira accounts associated with users: Verifies that all Jira accounts have been linked to users within Vanta. ✓

Slack accounts associated with users: Verifies that all Slack accounts have been linked to users within Vanta. ✓

1 DOCUMENT

Proof of completed access review ✓

► Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

1 TEST

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed within the specified SLA. ✓

2 DOCUMENTS

Employee termination checklist ✓

Employee termination security policy ✓

► Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

4 TESTS

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

CC 6.3

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.

5 CONTROLS

► Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

2 TESTS

Employees agree to System Access Control Policy: Verifies that all relevant employees have agreed to the System Access Control Policy. ✓

Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta. ✓

1 DOCUMENT

Access request ticket and history ✓

► Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

3 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

Least privileged policy for user data access: Verifies that the System Access Control Policy is in place and has been approved within Vanta. ✓

1 DOCUMENT

Access request ticket and history ✓

► Access reviews conducted

✓ COMPLETE

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

9 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

GitHub accounts associated with users: Verifies that all GitHub accounts have been linked to users within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that Google Workspace, Office 365, or Okta has been linked to Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Jira accounts associated with users: Verifies that all Jira accounts have been linked to users within Vanta. ✓

Slack accounts associated with users: Verifies that all Slack accounts have been linked to users within Vanta. ✓

1 DOCUMENT

Proof of completed access review ✓

► Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

1 TEST

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed within the specified SLA.

✓

2 DOCUMENTS

Employee termination checklist

✓

Employee termination security policy

✓

► Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

4 TESTS

Password policy configured for infrastructure (Heroku): This feature is built into Heroku.

✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku.

✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines.

✓

CC 6.4

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

4 CONTROLS

► Access reviews conducted

✓ COMPLETE

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

9 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

GitHub accounts associated with users: Verifies that all GitHub accounts have been linked to users within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that Google Workspace, Office 365, or Okta has been linked to Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Jira accounts associated with users: Verifies that all Jira accounts have been linked to users within Vanta. ✓

Slack accounts associated with users: Verifies that all Slack accounts have been linked to users within Vanta. ✓

1 DOCUMENT

Proof of completed access review ✓

► Data center access reviewed

✓ COMPLETE

The company reviews access to the data centers at least annually.

2 TESTS

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta. ✓

► Physical access processes established ✓ COMPLETE

The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.

2 TESTS

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta. ✓

► Visitor procedures enforced ✓ COMPLETE

The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.

2 TESTS

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta. ✓

CC 6.5

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.

4 CONTROLS

► Access revoked upon termination ✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

1 TEST

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed within the specified SLA. ✓

2 DOCUMENTS

Employee termination checklist ✓

Employee termination security policy ✓

▶ Asset disposal procedures utilized ✓ COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

1 TEST

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy. ✓

1 DOCUMENT

Proof of media/device disposal ✓

▶ Customer data deleted upon leave ✓ COMPLETE

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

1 TEST

Deleting from a logging bucket requires MFA: Verifies that all AWS S3 buckets used as the destination for CloudTrail or S3 access logs require MFA to delete. ✓

1 DOCUMENT

Customer data deletion record ✓

▶ Data retention procedures established ✓ COMPLETE

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

4 TESTS

Company has a Data Protection Policy: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Employees agree to Data Deletion Policy: Verifies that all relevant employees have agreed to the Data Deletion Policy. ✓

Employees agree to Data Protection Policy: Verifies that all relevant employees have agreed to the Data Protection Policy. ✓

Company has a Data Deletion Policy: Verifies that the Data Deletion Policy is in place and has been approved within Vanta. ✓

CC 6.6

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

9 CONTROLS

► Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

7 TESTS

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Strong SSL/TLS ciphers used: Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

SSL configuration has no known issues: Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

► Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

1 TEST

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

► Network and system hardening standards maintained

✓ COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

10 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA.

✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week.

✓

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached.

✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku.

✓

Firewall default disallows traffic: This feature is built into AWS.

✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku.

✓

Public SSH denied: Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22.

✓

Public SSH denied (Heroku): This feature is built into Heroku.

✓

Personal firewalls required: Verifies that management has approved the Asset Management Policy and that they have confirmed in Vanta that the policy requires use of a personal firewall.

✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

✓

► Network firewalls reviewed

✓ COMPLETE

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

7 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached.

✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku.

✓

Firewall default disallows traffic: This feature is built into AWS.

✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku.

✓

Public SSH denied: Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22.

✓

Public SSH denied (Heroku): This feature is built into Heroku.

✓

Personal firewalls required: Verifies that management has approved the Asset Management Policy and that they have confirmed in Vanta that the policy requires use of a personal firewall.

✓

► Network firewalls utilized

✓ COMPLETE

The company uses firewalls and configures them to prevent unauthorized access.

7 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied: Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Personal firewalls required: Verifies that management has approved the Asset Management Policy and that they have confirmed in Vanta that the policy requires use of a personal firewall. ✓

► Remote access encrypted enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

2 TESTS

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

► Remote access MFA enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

5 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

MFA on Google Workspace: Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled. ✓

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled. ✓

Company requires MFA where possible: Verifies that management has approved the Password Policy and that they have confirmed in Vanta that the plan requires multi-factor authentication on all accounts. ✓

► Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA.



Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker.



Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker.



Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag.



2 DOCUMENTS

Sample of remediated vulnerabilities



Vulnerability scan



► Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

4 TESTS

Password policy configured for infrastructure (Heroku): This feature is built into Heroku.



SSL/TLS on admin page of infrastructure console: This feature is built into AWS.



SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku.



Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines.



CC 6.7

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.

3 CONTROLS

► Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

7 TESTS

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Strong SSL/TLS ciphers used: Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

SSL configuration has no known issues: Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

► MDM system utilized

✓ COMPLETE

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed. ✓

► Portable media encrypted

✓ COMPLETE

The company encrypts portable and removable media devices when used.

1 TEST

Company has a Cryptography Policy: Verifies that the Cryptography Policy is in place and has been approved within Vanta. ✓

1 DOCUMENT

Removable media encryption ✓

CC 6.8

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

▶ Anti-malware technology utilized

✓ COMPLETE

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

1 TEST

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.

✓

▶ Development lifecycle established

✓ COMPLETE

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

2 TESTS

Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta.

✓

Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy.

✓

▶ Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA.

✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker.

✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker.

✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag.

✓

2 DOCUMENTS

Sample of remediated vulnerabilities

✓

Vulnerability scan

✓

System Operations

CC 7.1

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.

5 CONTROLS	
► Change management procedures enforced	✓ COMPLETE
The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	
1 TEST	
Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories.	✓
1 DOCUMENT	
CI/CD system in use	✓
► Configuration management system established	✓ COMPLETE
The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	
1 DOCUMENT	
CI/CD system in use	✓
► Risks assessments performed	✓ COMPLETE
The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	
1 TEST	
Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months.	✓

► Vulnerabilities scanned and remediated ✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

► Vulnerability and system monitoring procedures established ✓ COMPLETE

The company's formal policies outline the requirements for the following functions related to IT / Engineering:

- vulnerability management;
- system monitoring.

2 TESTS

Company has an approved Vulnerability Management Policy: Verifies that a Vulnerability Management Policy has been created and approved within Vanta. ✓

Employees agree to Vulnerability Management Policy: Verifies that all relevant employees have agreed to the Vulnerability Management Policy. ✓

CC 7.2

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.

7 CONTROLS

► Infrastructure performance monitored

✓ COMPLETE

An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

11 TESTS

Load balancer used (Heroku): This feature is built into Heroku.



Load balancer unhealthy host count monitored (AWS): Verifies that host health for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `UnHealthyHostCount` - `HealthyHostCount` - `EnvironmentHealth`



Load balancer latency monitored: Verifies that latency for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `Latency` - `EnvironmentHealth` - `ApplicationLatencyP99` - `ApplicationLatencyP95` - `TargetResponseTime`



Load balancer server errors monitored (AWS): Verifies that errors for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `HTTPCode_ELB_5XX` - `HTTPCode_ELB_5XX_Count` - `HTTPCode_Backend_5XX` - `HTTPCode_Target_5XX_Count` - `ApplicationRequests5xx`



SQL database CPU monitored: Verifies that all Amazon RDS instances enabled have a CloudWatch alarm enabled on the CPUUtilization metric.



SQL database freeable memory monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for the FreeableMemory metric.



Database IO monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for at least one of the following metrics: - `DiskQueueDepth` - `VolumeWriteIOPS` - `VolumeReadIOPS` - `WriteIOPS` - `ReadIOPS`



SQL database free storage space monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set up for at least one of the following metrics: - `FreeStorageSpace` on MySQL and PostgreSQL databases - `FreeLocalStorage` on Aurora MySQL and Aurora PostgreSQL databases - `AuroraVolumeBytesLeftTotal` on Aurora MySQL Databases



Serverless function error rate monitored (AWS): Verifies that all AWS Lambda functions have a CloudWatch alarm enabled on the Error metric.



Server CPU monitored (AWS): Verifies that all AWS EC2 instances have a CloudWatch alarm enabled on the `CPUUtilization` metric.



Messaging queue message age monitored: Verifies that all AWS SQS queues have a CloudWatch alarm set for the `ApproximateAgeOfOldestMessage` metric.



► Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

1 TEST

User activity and API use is tracked (Heroku): This feature is built into Heroku.



► Log management utilized

✓ COMPLETE

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.

6 TESTS

Heroku logs archived for 365 days: Verifies that all Heroku apps are using a plugin that stores logs for 365 days, or are using a custom log drain. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Only authorized users can access logging buckets: Verifies that no AWS S3 logging buckets grant access to the built-in AWS groups AllUsers or AuthenticatedUsers ✓

S3 server access logs enabled: Verifies there is at least one AWS S3 bucket acting as a destination for server access logging or CloudTrail data event logging. ✓

Server logs retained for 365 days (AWS): Verifies that all AWS CloudWatch Log Groups are configured to retain logs for at least 365 days. ✓

► Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

1 TEST

Records of penetration testing: Verifies that a periodic penetration test has been conducted recently and that evidence of that test has been uploaded to Vanta. ✓

2 DOCUMENTS

Penetration test report ✓

Penetration test remediation ✓

► Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA.



Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker.



Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker.



Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag.



2 DOCUMENTS

Sample of remediated vulnerabilities



Vulnerability scan



► Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA.



Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag.



2 DOCUMENTS

Sample of remediated vulnerabilities



Vulnerability scan



► Vulnerability and system monitoring procedures established ✓ COMPLETE

The company's formal policies outline the requirements for the following functions related to IT / Engineering:

- vulnerability management;
- system monitoring.

2 TESTS

Company has an approved Vulnerability Management Policy: Verifies that a Vulnerability Management Policy has been created and approved within Vanta. ✓

Employees agree to Vulnerability Management Policy: Verifies that all relevant employees have agreed to the Vulnerability Management Policy. ✓

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 objectives (security incidents) and, if so, takes actions to prevent or address such failures.

2 CONTROLS

► Incident management procedures followed ✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

SLA for security bugs: Verifies that management has approved the Change Management Policy and that they have set an SLA on P0 security issues within Vanta. ✓

► Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

Company Incident Response Plan cites responsible team members: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan names specific team members who are responsible for monitoring and responding to incidents. ✓

CC 7.4

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

5 CONTROLS

► Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

SLA for security bugs: Verifies that management has approved the Change Management Policy and that they have set an SLA on P0 security issues within Vanta. ✓

► Incident response plan tested

✓ COMPLETE

The company tests their incident response plan at least annually.

3 TESTS

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

► Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

Company Incident Response Plan cites responsible team members: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan names specific team members who are responsible for monitoring and responding to incidents. ✓

► Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

► Vulnerabilities scanned and remediated ✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

CC 7.5

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

4 CONTROLS

► Continuity and disaster recovery plans tested ✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

SLA for security bugs: Verifies that management has approved the Change Management Policy and that they have set an SLA on P0 security issues within Vanta. ✓

► Incident response plan tested

✓ COMPLETE

The company tests their incident response plan at least annually.

3 TESTS

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

► Incident response policies established

✓ COMPLETE

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

5 TESTS

Employees agree to Incident Response Plan: Verifies that all relevant employees have agreed to the Incident Response Plan. ✓

Policies for tracking follow-ups to important security items: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about tracking follow-ups after incidents. ✓

Incident Response Policy includes Lessons Learned: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan includes language about writing lessons learned after incidents. ✓

Company has an Incident Response Plan: Verifies that the Incident Response Plan is in place and has been approved within Vanta. ✓

Company Incident Response Plan cites responsible team members: Verifies that management has approved the Incident Response Plan and that they have confirmed in Vanta that the plan names specific team members who are responsible for monitoring and responding to incidents. ✓

Change Management

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

7 CONTROLS		
►	Change management procedures enforced	✓ COMPLETE
The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.		
1 TEST		
	Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories.	✓
1 DOCUMENT		
	CI/CD system in use	✓
►	Development lifecycle established	✓ COMPLETE
The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.		
2 TESTS		
	Company has a Change Management Policy: Verifies that the Change Management Policy is in place and has been approved within Vanta.	✓
	Employees agree to Change Management Policy: Verifies that all relevant employees have agreed to the Change Management Policy.	✓

► Network and system hardening standards maintained ✓ COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

10 TESTS

Infrastructure accounts allocated within one week of request: Verifies all tasks in the linked task tracker that are labeled with either `account-create` or `infra-change` tag were closed within the specified SLA. ✓

GitHub accounts allocated within one week of request: Verifies that all tasks tagged with `account-create` and `github` tags are closed within one week. ✓

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied: Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Personal firewalls required: Verifies that management has approved the Asset Management Policy and that they have confirmed in Vanta that the policy requires use of a personal firewall. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

► Penetration testing performed ✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

1 TEST

Records of penetration testing: Verifies that a periodic penetration test has been conducted recently and that evidence of that test has been uploaded to Vanta. ✓

2 DOCUMENTS

Penetration test report ✓

Penetration test remediation ✓

► Production deployment access restricted ✓ COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

2 TESTS

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch for all linked version control repositories. ✓

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days. ✓

► Service infrastructure maintained ✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

4 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

► Vulnerabilities scanned and remediated ✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

2 TESTS

Vulnerabilities identified in container packages are addressed (AWS): Verifies that all vulnerabilities detected by AWS container scanning are resolved within the specified SLA. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

Sample of remediated vulnerabilities ✓

Vulnerability scan ✓

Risk Mitigation

CC 9.1

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

4 CONTROLS		
▶	Continuity and Disaster Recovery plans established	✓ COMPLETE
The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.		
4 TESTS		
	Company has a Business Continuity Plan: Verifies that the Business Continuity Plan is in place and has been approved within Vanta.	✓
	Company has a Disaster Recovery Plan: Verifies that the Disaster Recovery Plan is in place and has been approved within Vanta.	✓
	Employees agree to Business Continuity Plan: Verifies that all relevant employees have agreed to the Business Continuity Plan.	✓
	Employees agree to Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Disaster Recovery Plan.	✓
▶	Cybersecurity insurance maintained	✓ COMPLETE
The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.		
1 DOCUMENT		
	Cybersecurity insurance policy document	✓
▶	Risk management program established	✓ COMPLETE
The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.		
2 TESTS		
	Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.	✓
	Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.	✓

► Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months.



CC 9.2

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

2 CONTROLS

► Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

1 TEST

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list.



3 DOCUMENTS

Cloud provider service agreement



Publicly available privacy policy



Publicly available terms of service



► Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

5 TESTS

Employees agree to Vendor Management Policy: Verifies that all relevant employees have agreed to the Vendor Management Policy.



Company has compliance security reports for critical vendors and reviews them annually: Verifies that all high risk vendors [Vendors](/vendors) have a completed security review in the past 12 months.



Policy to collect sub-service organization compliance reports: Verifies that management has approved the Vendor Management Policy and that the policy states that compliance reports are collected from external vendors.



Company has a Vendor Management Policy: Verifies that the Vendor Management Policy is in place and has been approved within Vanta.



Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list.



Additional Criteria for Availability

A 1.1

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.

2 CONTROLS

► Infrastructure performance monitored

✓ COMPLETE

An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

11 TESTS

Load balancer used (Heroku): This feature is built into Heroku.



Load balancer unhealthy host count monitored (AWS): Verifies that host health for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `UnHealthyHostCount` - `HealthyHostCount` - `EnvironmentHealth`



Load balancer latency monitored: Verifies that latency for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `Latency` - `EnvironmentHealth` - `ApplicationLatencyP99` - `ApplicationLatencyP95` - `TargetResponseTime`



Load balancer server errors monitored (AWS): Verifies that errors for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `HTTPCode_ELB_5XX` - `HTTPCode_ELB_5XX_Count` - `HTTPCode_Backend_5XX` - `HTTPCode_Target_5XX_Count` - `ApplicationRequests5xx`



SQL database CPU monitored: Verifies that all Amazon RDS instances enabled have a CloudWatch alarm enabled on the CPUUtilization metric.



SQL database freeable memory monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for the FreeableMemory metric.



Database IO monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for at least one of the following metrics: - `DiskQueueDepth` - `VolumeWriteIOPs` - `VolumeReadIOPs` - `WriteIOPs` - `ReadIOPs`



SQL database free storage space monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set up for at least one of the following metrics: - `FreeStorageSpace` on MySQL and PostgreSQL databases - `FreeLocalStorage` on Aurora MySQL and Aurora PostgreSQL databases - `AuroraVolumeBytesLeftTotal` on Aurora MySQL Databases



Serverless function error rate monitored (AWS): Verifies that all AWS Lambda functions have a CloudWatch alarm enabled on the Error metric.



Server CPU monitored (AWS): Verifies that all AWS EC2 instances have a CloudWatch alarm enabled on the `CPUUtilization` metric.



Messaging queue message age monitored: Verifies that all AWS SQS queues have a CloudWatch alarm set for the `ApproximateAgeOfOldestMessage` metric.



► System capacity reviewed

✓ COMPLETE

The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.

11 TESTS

Load balancer used (Heroku): This feature is built into Heroku.



Load balancer unhealthy host count monitored (AWS): Verifies that host health for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `UnHealthyHostCount` - `HealthyHostCount` - `EnvironmentHealth`



Load balancer latency monitored: Verifies that latency for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `Latency` - `EnvironmentHealth` - `ApplicationLatencyP99` - `ApplicationLatencyP95` - `TargetResponseTime`



Load balancer server errors monitored (AWS): Verifies that errors for all AWS load balancers are monitored via AWS CloudWatch using at least one of the following metrics: - `HTTPCode_ELB_5XX` - `HTTPCode_ELB_5XX_Count` - `HTTPCode_Backend_5XX` - `HTTPCode_Target_5XX_Count` - `ApplicationRequests5xx`



SQL database CPU monitored: Verifies that all Amazon RDS instances enabled have a CloudWatch alarm enabled on the CPUUtilization metric.



SQL database freeable memory monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for the FreeableMemory metric.



Database IO monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for at least one of the following metrics: - `DiskQueueDepth` - `VolumeWriteIOPS` - `VolumeReadIOPS` - `WriteIOPS` - `ReadIOPS`



SQL database free storage space monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set up for at least one of the following metrics: - `FreeStorageSpace` on MySQL and PostgreSQL databases - `FreeLocalStorage` on Aurora MySQL and Aurora PostgreSQL databases - `AuroraVolumeBytesLeftTotal` on Aurora MySQL Databases



Serverless function error rate monitored (AWS): Verifies that all AWS Lambda functions have a CloudWatch alarm enabled on the Error metric.



Server CPU monitored (AWS): Verifies that all AWS EC2 instances have a CloudWatch alarm enabled on the `CPUUtilization` metric.



Messaging queue message age monitored: Verifies that all AWS SQS queues have a CloudWatch alarm set for the `ApproximateAgeOfOldestMessage` metric.



1 DOCUMENT

Enabled automated log alerting



A 1.2

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.

9 CONTROLS

► Backup processes established ✓ COMPLETE

The company's data backup policy documents requirements for backup and recovery of customer data.

2 TESTS

Company has a Backup Policy: Verifies that the Backup Policy is in place and has been approved within Vanta. ✓

Employees agree to Backup Policy: Verifies that all relevant employees have agreed to the Backup Policy. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Continuity and disaster recovery plans tested ✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Database replication utilized ✓ COMPLETE

The company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails.

2 TESTS

Daily RDS database backups enabled (AWS): Verifies that all Amazon RDS instances have backups enabled. ✓

Daily database backups (Heroku): Verifies that all Heroku databases are backed up daily. This feature is automatically provided by Heroku Postgres plans on at least the Standard tier. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Environmental monitoring devices implemented ✓ COMPLETE

The company has environmental monitoring devices in place and configured to automatically generate an alert to management for environmental incidents.

2 TESTS

Company has compliance security reports for critical vendors and reviews them annually: Verifies that all high risk vendors [Vendors](/vendors) have a completed security review in the past 12 months. ✓

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list. ✓

► Environmental security inspected ✓ COMPLETE

The company has maintenance inspections of environmental security measures at the company data centers performed at least annually.

2 TESTS

Employees agree to Physical Security Policy: Verifies that all relevant employees have agreed to the Physical Security Policy. ✓

Company has a Physical Security Policy: Verifies that the Physical Security Policy is in place and has been approved within Vanta. ✓

► Production data backups conducted ✓ COMPLETE

The company performs periodic backups for production data. Data is backed up to a different location than the production system.

3 TESTS

Daily RDS database backups enabled (AWS): Verifies that all Amazon RDS instances have backups enabled. ✓

Daily database backups (Heroku): Verifies that all Heroku databases are backed up daily. This feature is automatically provided by Heroku Postgres plans on at least the Standard tier. ✓

Storage buckets versioned: Verifies that all AWS S3 buckets marked as containing user data have versioning enabled. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Production multi-availability zones established ✓ COMPLETE

The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.

1 DOCUMENT

Network diagram ✓

► Risk management program established

✓ COMPLETE

The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

2 TESTS

Employees agree to Risk Assessment Program: Verifies that all relevant employees have agreed to the Risk Assessment Program.

✓

Policies for risk assessment and management: Verifies that the Risk Assessment Policy is in place and has been approved within Vanta.

✓

► Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a Risk Assessment was completed within the last 12 months.

✓

A 1.3

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

4 CONTROLS

► Backup processes established

✓ COMPLETE

The company's data backup policy documents requirements for backup and recovery of customer data.

2 TESTS

Company has a Backup Policy: Verifies that the Backup Policy is in place and has been approved within Vanta.

✓

Employees agree to Backup Policy: Verifies that all relevant employees have agreed to the Backup Policy.

✓

1 DOCUMENT

Tabletop disaster recovery exercise

✓

► Continuity and Disaster Recovery plans established ✓ COMPLETE

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.

4 TESTS

Company has a Business Continuity Plan: Verifies that the Business Continuity Plan is in place and has been approved within Vanta. ✓

Company has a Disaster Recovery Plan: Verifies that the Disaster Recovery Plan is in place and has been approved within Vanta. ✓

Employees agree to Business Continuity Plan: Verifies that all relevant employees have agreed to the Business Continuity Plan. ✓

Employees agree to Disaster Recovery Plan: Verifies that all relevant employees have agreed to the Disaster Recovery Plan. ✓

► Continuity and disaster recovery plans tested ✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

► Intrusion detection system utilized ✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

1 TEST

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

Additional Criteria for Confidentiality

C 1.1

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

5 CONTROLS

► Data classification policy established ✓ COMPLETE

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

2 TESTS

Company has a Data Classification Policy: Verifies that the Data Classification Policy is in place and has been approved within Vanta. ✓

Employees agree to Data Classification Policy: Verifies that all relevant employees have agreed to the Data Classification Policy. ✓

► Data retention procedures established ✓ COMPLETE

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

4 TESTS

Company has a Data Protection Policy: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

Employees agree to Data Deletion Policy: Verifies that all relevant employees have agreed to the Data Deletion Policy. ✓

Employees agree to Data Protection Policy: Verifies that all relevant employees have agreed to the Data Protection Policy. ✓

Company has a Data Deletion Policy: Verifies that the Data Deletion Policy is in place and has been approved within Vanta. ✓

► Production data segmented ✓ COMPLETE

The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.

1 TEST

Policies cover employee access to user data: Verifies that the Data Protection Policy is in place and has been approved within Vanta. ✓

► Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

1 TEST

Vendors list maintained: Verifies that at least one external vendor has been added to the vendors list.

✓

3 DOCUMENTS

Cloud provider service agreement

✓

Publicly available privacy policy

✓

Publicly available terms of service

✓

► Unique account authentication enforced

✓ COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

10 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached.

✓

Employees have unique email accounts: Verifies that every linked identity provider has more than one user.

✓

Employees have unique version control accounts: Verifies that every linked version control account has more than one user.

✓

Service accounts used: Verifies that every AWS account is assigned a role.

✓

Service accounts used (Heroku): This feature is built into Heroku.

✓

Root infrastructure account unused: Verifies that the AWS root account has not been used in the last 30 days.

✓

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days.

✓

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users.

✓

No user account has a policy attached directly (Heroku): This feature is built into Heroku.

✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines.

✓

C 1.2

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

▶ Asset disposal procedures utilized

✓ COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

1 TEST

Employees agree to Asset Management Policy: Verifies that all relevant employees have agreed to the Asset Management Policy.

✓

1 DOCUMENT

Proof of media/device disposal

✓

▶ Customer data deleted upon leave

✓ COMPLETE

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

1 TEST

Deleting from a logging bucket requires MFA: Verifies that all AWS S3 buckets used as the destination for CloudTrail or S3 access logs require MFA to delete.

✓

1 DOCUMENT

Customer data deletion record

✓

Appendix A: Definitions

Bug bounty program: A crowdsourcing initiative that rewards individuals for discovering and reporting software bugs, especially those that could cause security vulnerabilities or breaches.

DDoS: Distributed denial of service. A DDoS attack is attack in which multiple compromised computer systems flood a target—such as a server, website, or other network resource—with messages or requests to cause a denial of service for users of the targeted resource.

Multifactor authentication (MFA): A security system that requires multiple methods of authentication using different types of credentials to verify users' identities before they can access a service.

Penetration test: The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker might exploit.

Principle of least privilege: The principle of giving a user or account only the privileges that are required to perform a job or necessary function.

Protected data: Data that is protected from public view or use; includes personally identifiable information, sensitive data, HIPAA data, or financial data.

Sensitive data: Any information a reasonable person considers private or would choose not to share with the public.

SSH: Secure shell. A cryptographic network protocol for operating network services securely over an unsecured network.

SSL: Secure sockets layer. The standard security technology for establishing an encrypted link between a web server and a browser.

Appendix B: Document history

Vanta continuously monitors the company's security and IT infrastructure to ensure the company complies with industry-standard security standards. Vanta tests the company's security posture continuously, and this report is automatically updated to reflect the latest findings.

About Vanta

[Vanta](#) provides a set of security and compliance tools that scan, verify, and secure a company's IT systems and processes. Our cloud-based technology identifies security flaws and privacy gaps in a company's security posture, providing a comprehensive view across cloud infrastructure, endpoints, corporate procedures, enterprise risk, and employee accounts.

Vanta is based in San Francisco, California.

