SAMPLE DOCUMENT. NOT A SOC 2 REPORT.

This is a sample document produced by cybersoftware to show the structure and depth of a SOC 2 report. The company described here does not exist. No CPA firm examined anything in this document, no opinion has been issued, and it attests to nothing. A real report carries the signed opinion of an independent licensed U.S. CPA firm, which appears in Section 1 and is absent here.

NORTHWIND EXAMPLE SYSTEMS, INC. (FICTIONAL)

SOC 2 Type 1 Report

FOR

Northwind Analytics Platform

TYPE 1 ASSESSMENT ON CONTROLS RELEVANT TO SECURITY

As-of Date: 31 March 2026

Document ID: SOC2-RPT-SAMPLEREPORT

Report Assembled: 28 September 2026

DRAFT. Not the issued report.

No independent service auditor has issued an opinion on this report.

SAMPLE

Table of Contents

Section 1	Independent Service Auditor's Report
Section 2	Management's Assertion & Required Disclosures
Section 2.1	Exceptions and Deficiencies
Section 3	Description of the System
Section 4	Trust Services Criteria, Related Controls, and Management's Status
Section 5	Disclosed Deviations and Deficiencies
Appendix A	Evidence Cross-Reference
Appendix B	Management Remediation Roadmap
Appendix C	Traceability

Each entry above links to its section. The PDF outline, shown as bookmarks in most PDF viewers, lists every section and appendix heading.

This report is intended solely for use by the management of Northwind Example Systems, Inc. (fictional), user entities of Northwind Example Systems, Inc. (fictional)'s services, and other parties who have sufficient knowledge and understanding of Northwind Example Systems, Inc. (fictional)'s services covered by this report. Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

SAMPLE

1. Independent Service Auditor's Report

No independent service auditor has yet issued an opinion on this report. This section will carry the signed opinion of the licensed CPA firm when the engagement is complete; until then every status in this document is management's own.

SAMPLE

2. Management's Assertion

Management of Northwind Example Systems, Inc. (fictional) (the “Company”) confirms, to the best of its knowledge and belief, that:

a. The accompanying description of the Northwind Analytics Platform system presents that system as designed and implemented as of 31 March 2026, in accordance with the description criteria for a description of a service organization’s system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (description criteria).
b. Except for the matters described in Section 2.1, the controls stated in the description were suitably designed as of 31 March 2026 to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria set forth in TSP section 100, *2017 Trust Services Criteria for Security* (applicable trust services criteria), if the controls operated effectively.

Management of Northwind Example Systems, Inc. (fictional) is responsible for:

c. Preparing the description and assertion.
d. Designing, implementing, and operating effective controls to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria.
e. Providing the service auditor with access to all information relevant to the description, assertion, and the examination, including records and documentation.

Security program approval: Asked “Has management formally approved the security and compliance program in the last 12 months?”, management answered “Yes” at intake. This is management’s representation, not a tested result.

Security roles and responsibilities: Asked “Are security roles and responsibilities documented and communicated?”, management answered “Yes” at intake. This is management’s representation, not a tested result.

SAMPLE

Subservice Organizations (Carve-Out)

The following subservice organizations are carved out of this examination; their controls are not covered by this report:

#	VENDOR / SERVICE
1	Amazon Web Services
2	Okta
3	GitHub
4	Datadog
5	Stripe
6	Linear

Section 3.7 describes the controls expected of them. The SOC 2 report or security attestation of each subservice organization is reviewed annually.

2.1 Exceptions and Deficiencies

51 findings from the intake questionnaire, the remediation record, and the roles disclosed by management. Each carries a reference used in Section 4, in Section 5 and in Appendix C, and, for the items still open, in Appendix B.

REF	CRITERIA	WHAT MANAGEMENT STATED	DEFICIENCY	STATUS	OWNER
F-01	CC6.4 Question A7c	Management stated "No" to: Are work areas with access to production systems or sensitive data separated from public or shared spaces?	Deficiency noted: work areas with production access are not separated from public or shared space.	Open	Priya Raman, Chief Technology Officer
F-02	CC1.3, CC2.2 Question B3	Management stated "Yes" to: Are security roles and responsibilities documented and communicated?	Supporting artifact not yet provided for documented security roles and responsibilities.	Open	Priya Raman, Chief Technology Officer
F-03	CC1.1 Question B4	Management stated "Yes" to: Do employees acknowledge a Code of Conduct?	Supporting artifact not yet provided for code of conduct acknowledgment.	Open	Priya Raman, Chief Technology Officer
F-04	CC1.2, CC4.1 Question B8	Management stated "Quarterly" to: How often does a body outside day-to-day management (a board, an advisory board, or a named independent advisor) review security matters?	Supporting artifact not yet provided for independent oversight of security.	Open	Priya Raman, Chief Technology Officer
F-05	CC1.5 Question B9	Management stated "Yes" to: Are security responsibilities included in performance expectations or job descriptions for staff with production access?	Supporting artifact not yet provided for security responsibilities in performance expectations.	Open	Priya Raman, Chief Technology Officer
F-06	CC9.2 Question C3	Management stated "Yes" to: Can you provide SOC reports or complete our risk questionnaire for each subservice org?	Supporting artifact not yet provided for SOC reports or risk questionnaires for subservice organizations.	Open	Priya Raman, Chief Technology Officer
F-07	CC9.2, CC4.1 Question C4	Management stated "Yes" to: Do you review the SOC 2 report or security attestation of each subservice organization annually?	Supporting artifact not yet provided for annual review of each subservice organization report.	Open	Priya Raman, Chief Technology Officer

SAMPLE

REF	CRITERIA	WHAT MANAGEMENT STATED	DEFICIENCY	STATUS	OWNER
F-08	CC3.1, CC3.2, CC3.3, CC3.4 Question E1	Management stated "No" to: Completed a formal information security risk assessment in the last 12 months?	Deficiency noted: no formal information security risk assessment has been completed in the last 12 months.	Open	Priya Raman, Chief Technology Officer
F-09	CC3.2 Question E2	Management stated "Spreadsheet or document" to: Where do you track identified risks and mitigation actions?	Supporting artifact not yet provided for risk register.	Open	Priya Raman, Chief Technology Officer
F-10	CC3.3 Question E4	Management stated "No" to: Does your risk assessment explicitly consider fraud and insider misuse?	Deficiency noted: no risk assessment explicitly considers fraud and insider misuse (see F-08).	Open	Priya Raman, Chief Technology Officer
F-11	CC3.4, CC5.1 Question E5	Management stated "Yes" to: Are significant changes (new systems, vendors, or headcount changes) assessed for risk before rollout?	Supporting artifact not yet provided for risk assessment of significant changes before rollout.	Open	Priya Raman, Chief Technology Officer
F-12	CC6.8, CC6.1 Question F3	Management stated "No" to: Do you use a device management tool (MDM/EDR) for company laptops?	Deficiency noted: no device management tool (mobile device management or endpoint detection and response) is used for company laptops.	Open	Priya Raman, Chief Technology Officer
F-13	CC6.8 Question F4	Management stated "Yes" to: Do all company laptops have endpoint protection installed and kept up to date?	Supporting artifact not yet provided for endpoint protection on laptops.	Open	Priya Raman, Chief Technology Officer
F-14	CC6.1, CC5.2, CC9.2 Question F6	Management stated "Yes" to: Do you maintain an inventory of production systems, data stores, and SaaS applications with an owner for each?	Supporting artifact not yet provided for inventory of production systems and applications with owners.	Open	Priya Raman, Chief Technology Officer
F-15	CC6.1, CC6.6 Question G1	Management stated "Yes" to: MFA required for cloud console access?	No supporting artifact for multi-factor authentication for cloud console access was on file at intake.	Remediated	Priya Raman, Chief Technology Officer
F-16	CC6.1, CC6.2, CC6.3 Question G4	Management stated "Yes" to: Role-based access for production systems?	Supporting artifact not yet provided for role-based access to production.	Open	Priya Raman, Chief Technology Officer

SAMPLE

REF	CRITERIA	WHAT MANAGEMENT STATED	DEFICIENCY	STATUS	OWNER
F-17	CC6.2, CC6.3 Question G7	Management stated "No" to: User access removed within 24 hours of termination?	Deficiency noted: user access is not removed within 24 hours of termination.	Open	Priya Raman, Chief Technology Officer
F-18	CC6.2, CC6.3, CC1.5 Question G8	Management stated "Annually" to: How often is a documented review of all user access to production performed?	Supporting artifact not yet provided for periodic review of user access to production.	Open	Priya Raman, Chief Technology Officer
F-19	CC6.2, CC6.3 Question G9	Management stated "No" to: Is access to production approved by a named manager before it is granted?	Deficiency noted: access to production is not approved by a named manager before it is granted.	Open	Priya Raman, Chief Technology Officer
F-20	CC1.4 Question H1	Management stated "Yes" to: Background checks completed before start?	Supporting artifact not yet provided for background checks before start.	Open	Priya Raman, Chief Technology Officer
F-21	CC1.1, CC1.4 Question H2	Management stated "Yes" to: NDA signed at hire?	Supporting artifact not yet provided for non-disclosure agreement at hire.	Open	Priya Raman, Chief Technology Officer
F-22	CC1.4, CC2.2 Question H3	Management stated "No" to: Security awareness training at hire and annually?	Deficiency noted: security awareness training is not completed both at hire and annually.	Open	Priya Raman, Chief Technology Officer
F-23	CC6.2, CC1.4 Question H4	Management stated "No" to: Do you follow a documented offboarding checklist that records access revocation for each departure?	Deficiency noted: no documented offboarding checklist records access revocation for each departure.	Open	Priya Raman, Chief Technology Officer
F-24	CC6.1 Question I1	Management stated "Confidential" to: Highest data classification level you apply.	Supporting artifact not yet provided for data classification scheme.	Open	Priya Raman, Chief Technology Officer
F-25	CC6.7 Question I2	Management stated "Yes" to: TLS for all external connections?	Supporting artifact not yet provided for TLS on all external connections.	Open	Priya Raman, Chief Technology Officer
F-26	CC6.1 Question I3	Management stated "Yes" to: Encryption at rest for databases and backups?	Supporting artifact not yet provided for encryption at rest for databases and backups.	Open	Priya Raman, Chief Technology Officer

SAMPLE

REF	CRITERIA	WHAT MANAGEMENT STATED	DEFICIENCY	STATUS	OWNER
F-27	CC6.5 Question I10	Management stated, in part, "Customer data is kept for the life of the contract plus 90 days, then deleted" (the full answer is in Appendix C), to: What is your retention period for customer data, and how is it securely disposed of at end of life?	No supporting artifact is on file for management's answer about any retention period and secure disposal method for customer data.	Open	Priya Raman, Chief Technology Officer
F-28	CC4.1, CC4.2, CC7.2 Question K1	Management stated "Yes" to: Centralized log collection for app and infrastructure?	Supporting artifact not yet provided for centralized log collection.	Open	Priya Raman, Chief Technology Officer
F-29	CC4.1, CC7.2 Question K2	Management stated "No" to: Admin/operator activity logged and reviewed weekly?	Deficiency noted: administrator and operator activity is not both logged and reviewed weekly.	Open	Priya Raman, Chief Technology Officer
F-30	CC7.2, CC7.3 Question K3	Management stated "Yes" to: Alerting configured for security events?	Supporting artifact not yet provided for alerting for security events.	Open	Priya Raman, Chief Technology Officer
F-31	CC6.6 Question L1	Management stated "Yes" to: WAF or equivalent in place?	Supporting artifact not yet provided for web application firewall.	Open	Priya Raman, Chief Technology Officer
F-32	CC7.1 Question M1	Management stated "No" to: Internal vulnerability scans run monthly?	Deficiency noted: internal vulnerability scans do not run monthly.	Open	Priya Raman, Chief Technology Officer
F-33	CC7.1, CC4.1 Question M3	Management stated "Yes" to: Penetration test performed annually?	Supporting artifact not yet provided for annual penetration test.	Open	Priya Raman, Chief Technology Officer
F-34	CC7.1 Question M4	Management stated "Yes" to: Critical patches applied within 30 days?	Supporting artifact not yet provided for critical patch service level.	Open	Priya Raman, Chief Technology Officer
F-35	CC7.1, CC5.2 Question M5	Management stated "Yes" to: Do you apply a documented hardening or configuration baseline to production systems?	Supporting artifact not yet provided for hardening or configuration baseline for production systems.	Open	Priya Raman, Chief Technology Officer
F-36	CC8.1 Question N1	Management stated "Yes" to: Changes tracked in a ticket or PR system?	No supporting artifact for change tracking in tickets or pull requests was on file at intake.	Remediated	Priya Raman, Chief Technology Officer
F-37	CC8.1 Question N2	Management stated "Yes" to: Peer review required before deploy?	Supporting artifact not yet provided for peer review before deployment.	Open	Priya Raman, Chief Technology Officer

SAMPLE

REF	CRITERIA	WHAT MANAGEMENT STATED	DEFICIENCY	STATUS	OWNER
F-38	CC8.1 Question N3	Management stated "Yes" to: Separate dev, test, and prod environments?	Supporting artifact not yet provided for separation of development, test and production environments.	Open	Priya Raman, Chief Technology Officer
F-39	CC8.1 Question N4	Management stated "No" to: Emergency change procedure documented?	Deficiency noted: no emergency change procedure is documented.	Open	Priya Raman, Chief Technology Officer
F-40	CC8.1 Question N5	Management stated "No" to: Are production deployments approved by someone other than the author?	Deficiency noted: production deployments are not approved by someone other than the author.	Open	Priya Raman, Chief Technology Officer
F-41	CC7.3, CC7.4, CC7.5 Question O1	Management stated "No" to: Incident Response Plan exists and is approved?	Deficiency noted: no approved incident response plan exists.	Open	Priya Raman, Chief Technology Officer
F-42	CC7.4, CC7.5 Question O3	Management stated "Yes" to: Root cause analysis performed for high-severity incidents?	Supporting artifact not yet provided for root cause analysis for high-severity incidents.	Open	Priya Raman, Chief Technology Officer
F-43	CC7.5, CC9.1 Question P1	Management stated "Yes" to: Databases and volumes backed up?	Supporting artifact not yet provided for backups of databases and volumes.	Open	Priya Raman, Chief Technology Officer
F-44	CC7.5, CC9.1 Question P4	Management stated "No" to: Multi-region or multi-zone recovery strategy?	Deficiency noted: no multi-region or multi-zone recovery strategy is in place.	Open	Priya Raman, Chief Technology Officer
F-45	CC7.5, CC9.1 Question P5	Management stated "No" to: DR/BCP tested at least annually?	Deficiency noted: no disaster recovery or business continuity plan test is performed at least annually.	Open	Priya Raman, Chief Technology Officer
F-46	CC9.2 Question Q1	Management stated "No" to: Vendor risk reviews performed before onboarding and yearly?	Deficiency noted: vendor risk reviews are not performed before onboarding and yearly.	Open	Priya Raman, Chief Technology Officer
F-47	CC2.3 Question Q2	Management stated "No" to: Customers informed of their complementary user entity controls?	Deficiency noted: customers are not informed of their complementary user entity controls.	Open	Priya Raman, Chief Technology Officer

SAMPLE

REF	CRITERIA	WHAT MANAGEMENT STATED	DEFICIENCY	STATUS	OWNER
F-48	CC9.2 Question Q3	Management stated, in part, "Amazon Web Services (hosting), Okta (identity), GitHub (source control)" (the full answer is in Appendix C), to: List each vendor with production data access, its criticality, and the date of its last review.	No supporting artifact is on file for management's answer about any vendors with production data access and the criticality and last review date of each.	Open	Priya Raman, Chief Technology Officer
F-49	CC1.2, CC4.1, CC5.3 Question R1	Management stated "Yes" to: Does management review the overall security and compliance program at least annually?	Supporting artifact not yet provided for annual management review of the security program.	Open	Priya Raman, Chief Technology Officer
F-50	CC4.2, CC5.3 Question R2	Management stated "Yes" to: Is there a process to track and close remediation items from audits, incidents, tests, or reviews?	Supporting artifact not yet provided for tracking and closing remediation items.	Open	Priya Raman, Chief Technology Officer
F-51	CC4.2, CC2.1 Question R4	Management stated, in part, "Anyone who finds a control deficiency files it in Linear with the security" (the full answer is in Appendix C), to: How are control deficiencies reported to management, and to whom?	No supporting artifact is on file for management's answer about any reporting of control deficiencies to management and who receives it.	Open	Priya Raman, Chief Technology Officer

Risks identified by management at intake

Stated by management in intake question E3.

“A prolonged AWS region outage. An ingestion pipeline fault that serves one customer another customer's data. Loss of the single engineer who owns the deployment path.”

SAMPLE

3. Description of the System

> **Controls not in place at the as-of date.** This description covers the system as management describes it. Where management reported during the readiness assessment that a control is not in place, it is listed once in Section 2.1 rather than repeated here, so that a reader counting exceptions counts each one exactly once.

Company Overview and Types of Products and Services

Northwind Example Systems builds an analytics platform for mid-market operations teams. The company is fictional and exists only in this sample.

Asked for a one-sentence mission for Northwind Analytics Platform, management answered "Give operations teams a dashboard they can trust without hiring a data team."

Northwind ingests customer operational data, models it, and serves dashboards, scheduled reports and a query API to mid-market operations teams.

Principal Service Commitments and System Requirements

Northwind Example Systems, Inc. (fictional) designs its processes and procedures for Northwind Analytics Platform to meet its objectives for that system. Those objectives are based both on the services that Northwind Example Systems, Inc. (fictional) provides to user entities and on the commitments Northwind Example Systems, Inc. (fictional) makes to user entities.

Management represents the following in support of its commitments to user entities:

- Service availability with a target of 99.9%.
- Transport Layer Security (TLS) is used for all external connections.
- Databases and backups are encrypted at rest.
- Role-based access is used for production systems.
- Management reviews the overall security and compliance program at least annually.

Components of the System Used to Provide the Service

The following table summarizes the five principal components of Northwind Example Systems, Inc. (fictional)'s system:

SAMPLE

COMPONENT	DESCRIPTION
Infrastructure	Production infrastructure hosted on AWS.
Software	The Northwind Analytics Platform application is deployed on AWS. The vendors listed at intake are named in 3.1.
People	The headcount management gave is quoted in 3.3. Security and compliance owner: Priya Raman, Chief Technology Officer.
Procedures	None of the 13 formal security policies is on file yet. Management reviews the overall security and compliance program at least annually.
Data	Customer data, configuration data, log data, and backup data processed by the system. Data is classified with levels up to Confidential.

3.1 Primary Infrastructure

Northwind Example Systems, Inc. (fictional) hosts Northwind Analytics Platform on cloud infrastructure. The following table lists the vendors named at intake and what each product is, in management's words where given:

SERVICE	CATEGORY	PURPOSE
Amazon Web Services	Cloud Hosting	Cloud infrastructure provider
Okta	Identity Provider	Identity and access management service
GitHub	Source Code Hosting	Source code hosting service
Datadog	Monitoring	Monitoring and observability platform
Stripe	Payments	Payment processing service
Linear	Project Management	Issue tracking and project management tool

Northwind Example Systems, Inc. (fictional)'s production infrastructure is hosted on AWS.

Encryption

Databases and backups are encrypted at rest. Asked for the encryption standard for data at rest, management answered "AES-256 (AWS KMS managed keys)". Transport Layer Security (TLS) is used for all external connections. Asked for the encryption standard for data in transit, management answered "TLS 1.3". Asked for the system used to manage encryption keys, management answered "AWS Key Management Service". Encryption keys are rotated every year.

3.2 Primary Software

The Northwind Analytics Platform application is deployed on AWS.

The following components were named at intake:

COMPONENT	TECHNOLOGY	PURPOSE
Application Runtime	AWS	Production cloud provider

SAMPLE

Application	Northwind Analytics Platform	The in-scope product
Identity Provider	Okta	Identity and access management service
Monitoring	Datadog	Monitoring and observability platform

Source code is hosted in GitHub. Changes are tracked in a ticket or pull request system. Peer review is required before deployment. Development, test, and production environments are separated.

3.3 People

Asked for its approximate headcount, management answered "18 employees and 3 contractors".

Asked for its functional areas or departments, management answered "Engineering. Founders cover Security. Support."

The following contacts were named at intake:

ROLE	CONTACT
Security Program Owner	Priya Raman, Chief Technology Officer
Executive Signatory	Marcus Webb, Chief Executive Officer
Security Contact	Priya Raman, Chief Technology Officer
Technical Contact	Tom Iyer

3.4 Processes and Procedures

The Northwind Analytics Platform application runs in AWS. No documented security policies are on file yet.

Environment Separation and Network Security

Development, test, and production environments are separated. Security groups or firewall rules restrict production ingress. A web application firewall (WAF) or equivalent is in place. Direct SSH or console access is limited to named administrators.

Security Program Review and Approval

Management reviews the overall security and compliance program at least annually. Management formally approved the security and compliance program within the last 12 months.

Risk Tracking

Identified risks and mitigation actions are tracked in a spreadsheet or document.

Security Roles

Security roles and responsibilities are documented and communicated.

Logical Access Controls

Account sharing is prohibited. Role-based access is used for production systems. Multi-factor authentication (MFA) is required for cloud console access.

SAMPLE

Change Management

Changes are tracked in a ticket or pull request system. Peer review is required before deployment.

3.5 Data

Northwind Example Systems, Inc. (fictional) classifies data with levels up to Confidential. The following data types are processed by Northwind Analytics Platform:

DATA TYPE	DESCRIPTION	PROTECTION
Configuration Data	Configuration of the production system and its services.	Access restricted by role
Customer Data	Customer data processed by Northwind Analytics Platform.	Encrypted at rest in databases and backups; TLS used for all external connections
Log Data	Application and infrastructure logs.	Collected centrally. Protections reported as not in place are listed in Section 2.1.
Backup Data	Databases and volumes are backed up with a daily differential backup and a weekly full backup.	Encrypted. Protections reported as not in place are listed in Section 2.1.

Removable media is not permitted.

Asked for any retention period and secure disposal method for customer data, management answered "Customer data is kept for the life of the contract plus 90 days, then deleted from the production database and from backups as they expire at 35 days. Laptops are wiped through device management before reissue."

3.6 System Boundaries

The system boundary for Northwind Analytics Platform encompasses all infrastructure, software, people, procedures, and data involved in delivering Northwind Example Systems, Inc. (fictional)'s services. The production environment is hosted on AWS.

Asked for its office locations in scope, management answered "One office in Austin, Texas. The rest of the team works remotely across the United States."

Northwind Example Systems, Inc. (fictional) operates from physical offices. Physical access controls at those locations are described under Physical Security and Environmental Controls.

Scope Confirmation: Management confirms that only the products and locations listed at intake are in scope. Management notes: "Only the Northwind Analytics Platform and the Austin office are in scope."

The following are **not** within the boundaries of the system in scope:

- The controls operated by the subservice organizations listed in Section 3.7, under the carve-out method
- Personal devices and equipment that Northwind Example Systems, Inc. (fictional) does not own

3.7 Third-Party Access and Subservice Organizations

The following vendors used in production were listed at intake:

SAMPLE

VENDOR	EXPECTED CONTROLS
Amazon Web Services	Physical security, infrastructure availability, separation of customer tenants on shared infrastructure.
Okta	Authentication service availability and security, identity federation, session token security.
GitHub	Platform access controls, platform audit logging, hosting infrastructure security.
Datadog	Ingestion pipeline security, storage security for monitoring data, platform access controls.
Stripe	Payment data encryption, payment infrastructure security.
Linear	Platform access controls, platform audit logging.

Carve-Out Method: The carve-out method is used for subservice organizations; the controls they operate are excluded from the scope of this description.

Evidence Plan: SOC reports or completed risk questionnaires can be provided for each subservice organization.

The SOC 2 report or security attestation of each subservice organization is reviewed annually.

Disclosures About Identified Security Incidents

Management is responsible for disclosing in this section any security incident identified as of 31 March 2026 that materially affected the system or the services provided to user entities.

Integrity and Ethical Values

Employees acknowledge a Code of Conduct. Asked for the scope and ethical standards its Code of Conduct covers, management answered "Conflicts of interest, acceptable use of company systems, confidentiality of customer data, and the duty to report a suspected security or ethics concern."

Asked for its whistleblower or ethics reporting channel, management answered "ethics@northwind.example". Asked for the management body responsible for reviewing Code of Conduct or ethics reports, management answered "The advisory board, at its quarterly meeting."

Commitment to Competence

Management did not represent any competence practices as in place at intake; those it reported as not in place are listed in Section 2.1.

Management's Philosophy and Operating Style

Management formally approved the security and compliance program within the last 12 months.

Organizational Structure

Northwind Example Systems, Inc. (fictional)'s security and compliance program is owned by Priya Raman, Chief Technology Officer.

SAMPLE

Asked for its functional areas or departments, management answered "Engineering. Founders cover Security. Support."

Security roles and responsibilities are documented and communicated. Security responsibilities are included in performance expectations or job descriptions for staff with production access.

A body outside day to day management reviews security matters every quarter. Asked which body or advisor it is, management answered "The Northwind advisory board".

Human Resource Policies and Practices

Management represents the following human resource practices:

- Background checks are completed before start.
- A non-disclosure agreement (NDA) is signed at hire.

Security Management

Priya Raman, Chief Technology Officer, owns Northwind Example Systems, Inc. (fictional)'s security and compliance program. An inventory of production systems, data stores and SaaS applications with an owner for each is maintained.

Security Policies

No information security policy is on file yet. The table lists the areas Northwind Example Systems, Inc. (fictional)'s policy set is to cover.

POLICY	STATUS
Access Control	Not yet generated
Asset Management	Not yet generated
Business Continuity and Disaster Recovery	Not yet generated
Code of Conduct	Not yet generated
Cryptography	Not yet generated
Data Management	Not yet generated
Human Resources Security	Not yet generated
Incident Response	Not yet generated
Information Security Policy	Not yet generated
Operations Security	Not yet generated
Risk Management	Not yet generated
Secure Development	Not yet generated
Third Party and Vendor Management	Not yet generated

SAMPLE

Personnel Security

Management represents the following personnel security measures:

- Background checks are completed before start.
- Security roles and responsibilities are documented and communicated.
- A non-disclosure agreement (NDA) is signed at hire.
- Employees acknowledge a Code of Conduct.

Physical Security and Environmental Controls

Northwind Example Systems, Inc. (fictional)'s production workloads run on AWS. Physical and environmental controls at AWS's data centers are the provider's responsibility.

Northwind Example Systems, Inc. (fictional) represents the following physical access controls at its office locations:

CONTROL	DESCRIPTION
Office Access Control	Access to the offices or coworking spaces is controlled by a badge or electronic access control system.
Visitor Escort Policy	Visitors are escorted and recorded when entering areas with company systems or records.

Endpoint and Device Controls

Management represents the following endpoint and device controls:

- An inventory of devices that access production data is maintained.
- Company laptops are configured with full disk encryption.
- Endpoint protection is installed and kept up to date on all company laptops.
- Users are required to lock their devices when unattended.

Change Management

Management represents the following change management practices:

- Changes are tracked in a ticket or pull request system.
- Peer review is required before deployment.
- Development, test, and production environments are separated.

System Monitoring

Management represents the following logging and monitoring practices:

- Application and infrastructure logs are collected centrally.
- Alerting is configured for security events.
- Capacity and uptime are monitored.

SAMPLE

Incident Management

Management represents the following incident management practices:

- Security events are logged with severity, date, and status.
- Root cause analysis is performed for high-severity incidents.

Data Backup and Recovery

Databases and volumes are backed up with a daily differential backup and a weekly full backup.

Backups are encrypted.

System Account Management

Management represents the following logical access practices:

- Multi-factor authentication (MFA) is required for cloud console access.
- Role-based access is used for production systems.
- A minimum password length of at least 12 characters is enforced.
- The password and authentication policy is enforced in Okta.
- Account sharing is prohibited.
- A documented review of all user access to production is performed every year.

The number of privileged administrators for production is 3.

Risk Management Program

Risk Assessment of Significant Changes

Significant changes are assessed for risk before rollout.

Principal Risks

Asked for the top risks to its service commitments, management answered "A prolonged AWS region outage. An ingestion pipeline fault that serves one customer another customer's data. Loss of the single engineer who owns the deployment path."

Vulnerability Management

Management represents the following vulnerability management practices:

- External vulnerability scans run at least quarterly.
- A penetration test is performed annually.
- Critical patches are applied within 30 days.
- A documented hardening or configuration baseline is applied to production systems.

Vendors with Production Data Access

Asked for any vendors with production data access and the criticality and last review date of each, management answered "Amazon Web Services (hosting), Okta (identity), GitHub (source control), Datadog (monitoring), Stripe (payments), Linear (change tracking)".

SAMPLE

Security Program Review, Remediation Tracking and Reporting of Control Deficiencies

Management represents the following security program review and remediation tracking practices:

- Management reviews the overall security and compliance program at least annually.
- There is a process to track and close remediation items from audits, incidents, tests or reviews.
- Remediation items are tracked in a ticketing system.

Asked for any reporting of control deficiencies to management and who receives it, management answered "Anyone who finds a control deficiency files it in Linear with the security label; the security owner reviews the list weekly and reports open items to the CEO at the monthly leadership meeting."

Information and Communications Systems

Internal Communications

Security roles and responsibilities are communicated.

External Communications

Transport Layer Security (TLS) is used for all external connections.

Asked for its support channel, management answered "support@northwind.example".

Uptime SLA target: 99.9%.

User entities have not yet been informed of their complementary user entity controls.

Security Testing and Third-Party Security Monitoring

Management represents the following security testing and subservice organization monitoring practices:

- A penetration test is performed annually.
- External vulnerability scans run at least quarterly.
- SOC reports or completed risk questionnaires can be provided for each subservice organization.
- The SOC 2 report or security attestation of each subservice organization is reviewed annually.

Complementary User Entity Controls (CUECs)

Northwind Example Systems, Inc. (fictional)'s system of internal controls is designed with the assumption that certain complementary controls will be implemented by user entities. The effectiveness of controls at Northwind Example Systems, Inc. (fictional) is dependent, in part, on the following controls being suitably designed and operating effectively at user entities:

CONTROL AREA	USER ENTITY RESPONSIBILITY
Access Management	User entities are responsible for managing any access they grant their personnel to Northwind Analytics Platform.
Authentication	User entities are responsible for safeguarding any credentials their personnel use to access Northwind Analytics Platform.
Data Classification	User entities are responsible for classifying their data before it is processed by Northwind Analytics Platform and for ensuring that the data they provide is appropriate for the intended use of Northwind Analytics Platform.

SAMPLE

Incident Notification	User entities are responsible for promptly notifying Northwind Example Systems, Inc. (fictional) of any suspected security incidents or unauthorized access related to their use of Northwind Analytics Platform.
Configuration Management	User entities are responsible for reviewing and configuring any security settings Northwind Analytics Platform makes available to them, in accordance with their own security policies.

Management represents that user entities have not yet been informed of their complementary user entity controls.

Complementary Subservice Organization Controls (CSOCs)

Northwind Example Systems, Inc. (fictional) uses the carve-out method to address subservice organizations. Controls operated by these organizations are excluded from the scope of this report; Northwind Example Systems, Inc. (fictional)'s reliance on those controls is documented in *Section 3.7. Third-Party Access and Subservice Organizations*, which lists each subservice organization and the controls expected of them.

The complementary subservice organization controls relied upon by Northwind Example Systems, Inc. (fictional) include physical and environmental safeguards at AWS data centers and the controls Section 3.7 lists as expected of each subservice organization. Northwind Example Systems, Inc. (fictional) reviews the SOC 2 report or security attestation of each subservice organization annually.

Disclosure of Significant Changes

No significant changes to the system, the services provided, or the controls in place were recorded as part of this description. Management is responsible for disclosing, before the report is issued, any significant change that would materially affect user entities.

Types of changes that would require disclosure include:

- Changes to the services provided to user entities, including new features, deprecated functionality, or modified service levels
- Significant changes to IT and security personnel, including key departures or reorganizations
- Significant changes to system processes, architecture, or applications that could affect security controls
- Changes to legal and regulatory requirements affecting the system or the services provided
- Changes to organizational structure affecting the control environment, including mergers, acquisitions, or divestitures

SAMPLE

4. Trust Services Criteria, Related Controls, and Management's Status

The following table lists each Common Criteria point of focus (CC1 to CC9, 197 points of focus) with the control management describes, the basis on file for it (intake answers, generated policies, and uploaded artifacts), the evidence reference into Appendix A, the responsible owner, and management's status. No independent service auditor has tested these controls. The status column is management's own and is derived from the intake questionnaire, the remediation record, and the artifacts on file.

> **Status summary.** Of 33 control points, 12 implemented per management, 0 remediated during readiness, 21 with an exception, 0 not applicable to this engagement, and 0 not assessed. Across the 197 points of focus below, 54 are operating, 0 remediated, 40 in exception, 0 not applicable, and 103 not assessed.

> **Basis summary.** Of 33 control points in scope, 1 supported by an artifact on file, 11 represented by management without a separate examination and 21 reported by management as not in place. A representation is management's own statement in the readiness assessment; it is recorded as such and was not separately examined.

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC1: Control Environment						
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.						
CC1.1A	Sets the Tone at the Top	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.1 (B2, B4, H2) do not address this point of focus; the evidence requests for code of conduct acknowledgment and non-disclosure agreement at hire are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.1B	Establishes Standards of Conduct	Employees acknowledge a Code of Conduct. A non-disclosure agreement (NDA) is signed at hire.	Management's answers on code of conduct acknowledgment and non-disclosure agreement at hire support this point of focus; the evidence requests for code of conduct acknowl-	--	Priya Raman, Chief Technology Officer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			edgment and non-disclosure agreement at hire are still open; no policy or artifact is on file.			
CC1.1C	Evaluates Adherence to Standards of Conduct	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.1 (B2, B4, H2) do not address this point of focus; the evidence requests for code of conduct acknowledgment and non-disclosure agreement at hire are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.1D	Addresses Deviations in a Timely Manner	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.1 (B2, B4, H2) do not address this point of focus; the evidence requests for code of conduct acknowledgment and non-disclosure agreement at hire are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.1E	Considers Contractors and Vendor Employees in Demonstrating Its Commitment	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.1 (B2, B4, H2) do not address this point of focus; the evidence requests for code of conduct acknowledgment and non-disclosure agreement at hire are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.						
CC1.2A	Establishes Oversight Responsibilities	Management formally approved the security and compliance program within the last 12	Management's answers on independent oversight of security and manage-	--	Priya Raman, Chief	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
		months. A body outside day to day management reviews security matters at least twice a year.	ment approval of the security program support this point of focus; the evidence requests for independent oversight of security and annual management review of the security program are still open; no policy or artifact is on file.		Technology Officer	
CC1.2B	Applies Relevant Expertise	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.2 (B2, B8, R1) do not address this point of focus; the evidence requests for independent oversight of security and annual management review of the security program are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.2C	Operates Independently	A body outside day to day management reviews security matters at least twice a year.	Management's answer on independent oversight of security supports this point of focus; the evidence requests for independent oversight of security and annual management review of the security program are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC1.2D	Supplements Board Expertise	A body outside day to day management reviews security matters at least twice a year.	Management's answer on independent oversight of security supports this point of focus; the evidence requests for independent oversight of security and annual management review of the security program are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.						
CC1.3A	Consider All Structures of the Entity	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.3 (B3) do not address this point of focus; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.3B	Establishes Reporting Lines	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.3 (B3) do not address this point of focus; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.3C	Defines, Assigns, and Limits Authorities and Responsibilities	Security roles and responsibilities are documented and communicated.	Management's answer on documented security roles and responsibilities supports this point of focus; the evidence request for documented security roles and responsibilities is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC1.3D	Addresses Specific Requirements When Defining Authorities and Responsibilities	Security roles and responsibilities are documented and communicated.	Management's answer on documented security roles and responsibilities supports this point of focus; the evidence request for documented security roles and responsibilities is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC1.3E	Consider Interactions With External Parties	Not addressed at intake: no intake question addresses this point of	No intake question addresses this point of focus; manage-	--	Priya Raman, Chief	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
	When Establishing Structures, Reporting Lines, Authorities, and Responsibilities	focus.	ment's intake answers under CC1.3 (B3) do not address this point of focus; the evidence request for documented security roles and responsibilities is still open.		Technology Officer	
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. Exception on this criterion as a whole: offboarding checklist recording access revocation (F-23). See Section 2.1.						
CC1.4A	Establishes Policies and Practices	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.4 (H1, H2, H3, H4) do not address this point of focus; the remediation items for offboarding checklist recording access revocation and security awareness training at hire and annually are still open; the evidence requests for background checks before start and nondisclosure agreement at hire are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.4B	Evaluates Competence and Addresses Shortcomings	Not in place per management: security awareness training at hire and annually (F-22 in Section 2.1).	Management answered No to security awareness training at hire and annually; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC1.4C	Attracts, Develops, and Retains Individuals	Not in place per management: security awareness training at hire and annually (F-22 in Section 2.1).	Management answered No to security awareness training at hire and annually; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC1.4D	Plans and Prepares for Succession	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.4 (H1, H2, H3, H4) do not address this	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			point of focus; the remediation items for offboarding checklist recording access revocation and security awareness training at hire and annually are still open; the evidence requests for background checks before start and non-disclosure agreement at hire are still open.			
CC1.4E	Considers the Background of Individuals	Background checks are completed before start.	Management's answer on background checks before start supports this point of focus; the remediation items for offboarding checklist recording access revocation and security awareness training at hire and annually are still open; the evidence requests for background checks before start and non-disclosure agreement at hire are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC1.4F	Considers the Technical Competency of Individuals	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.4 (H1, H2, H3, H4) do not address this point of focus; the remediation items for offboarding checklist recording access revocation and security awareness training at hire and annually are still open; the evidence requests for background checks before start and non-	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			disclosure agreement at hire are still open.			
CC1.4G	Provides Training to Maintain Technical Competencies	Not in place per management: security awareness training at hire and annually (F-22 in Section 2.1).	Management answered No to security awareness training at hire and annually; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.						
CC1.5A	Enforces Accountability Through Structures, Authorities, and Responsibilities	Security responsibilities are included in performance expectations or job descriptions for staff with production access.	Management's answer on security responsibilities in performance expectations supports this point of focus; the evidence requests for periodic review of user access to production and security responsibilities in performance expectations are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC1.5B	Establishes Performance Measures, Incentives, and Rewards	Security responsibilities are included in performance expectations or job descriptions for staff with production access.	Management's answer on security responsibilities in performance expectations supports this point of focus; the evidence requests for periodic review of user access to production and security responsibilities in performance expectations are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC1.5C	Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.5 (B9, G8) do not address this point of focus; the evidence requests for periodic review of user access to production and security respon-	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			sibilities in performance expectations are still open.			
CC1.5D	Considers Excessive Pressures	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC1.5 (B9, G8) do not address this point of focus; the evidence requests for periodic review of user access to production and security responsibilities in performance expectations are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC1.5E	Evaluates Performance and Rewards or Disciplines Individuals	Security responsibilities are included in performance expectations or job descriptions for staff with production access.	Management's answer on security responsibilities in performance expectations supports this point of focus; the evidence requests for periodic review of user access to production and security responsibilities in performance expectations are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC2: Communication and Information						
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.						
CC2.1A	Identifies Information Requirements	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC2.1B	Captures Internal and External Sources of Data	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.1C	Processes Relevant Data Into Information	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.1D	Maintains Quality Throughout Processing	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.1E	Documents Data Flow	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC2.1F	Manages Assets	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.1G	Classifies Information	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.1H	Uses Information That Is Complete and Accurate	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.1I	Manages the Location of Assets	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.1 (R4) do not address this point of focus; the evidence request for any reporting of control deficiencies to management and who receives it is still open.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.						
CC2.2A	Communicates Internal Control Information	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.2B	Communicates With the Board of Directors	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.2C	Provides Separate Communication Lines	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.2D	Selects Relevant Method of Communication	Not addressed at intake: no intake question addresses this point of	No intake question addresses this point of focus; management's intake an-	--	Priya Raman, Chief	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
		focus.	swers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open.		Technology Officer	
CC2.2E	Communicates Responsibilities	Security roles and responsibilities are documented and communicated.	Management's answer on documented security roles and responsibilities supports this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC2.2F	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.2G	Communicates Objectives and Changes to Objectives	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			is still open; the evidence request for documented security roles and responsibilities is still open.			
CC2.2H	Communicates Information to Improve Security Knowledge and Awareness	Not in place per management: security awareness training at hire and annually (F-22 in Section 2.1).	Management answered No to security awareness training at hire and annually; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC2.2K	Communicates Information About System Operation and Boundaries	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.2L	Communicates System Objectives	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually is still open; the evidence request for documented security roles and responsibilities is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.2M	Communicates System Changes	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.2 (B3, H3) do not address this point of focus; the remediation item for security awareness training at hire and annually	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			is still open; the evidence request for documented security roles and responsibilities is still open.			
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.						
CC2.3A	Communicates to External Parties	Not in place per management: communication of complementary user entity controls (F-47 in Section 2.1).	Management answered No to communication of complementary user entity controls; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC2.3B	Enables Inbound Communications	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.3 (Q2) do not address this point of focus; the remediation item for communication of complementary user entity controls is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.3C	Communicates With the Board of Directors	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.3 (Q2) do not address this point of focus; the remediation item for communication of complementary user entity controls is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.3D	Provides Separate Communication Lines	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.3 (Q2) do not address this point of focus; the remediation item for communication of complementary user entity controls is still open.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC2.3E	Selects Relevant Method of Communication	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.3 (Q2) do not address this point of focus; the remediation item for communication of complementary user entity controls is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.3I	Communicates Information About System Operation and Boundaries	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.3 (Q2) do not address this point of focus; the remediation item for communication of complementary user entity controls is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.3J	Communicates System Objectives	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.3 (Q2) do not address this point of focus; the remediation item for communication of complementary user entity controls is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC2.3K	Communicates System Responsibilities	Not in place per management: communication of complementary user entity controls (F-47 in Section 2.1).	Management answered No to communication of complementary user entity controls; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC2.3L	Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC2.3 (Q2) do not address this point of focus; the remediation item for communication	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			of complementary user entity controls is still open.			
CC3: Risk Assessment						
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.						
CC3.1A	Reflects Management's Choices	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1B	Considers Tolerances for Risk	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1C	Includes Operations and Financial Performance Goals	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1D	Forms a Basis for Committing of Resources	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk as-	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			sessment in the last 12 months is still open.			
CC3.1H	Complies With Externally Established Frameworks	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1I	Considers the Required Level of Precision	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1J	Reflects Entity Activities	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1K	Reflects Management's Choices (Internal)	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1L	Considers the Required Level of Precision	Not addressed at intake: no intake question addresses this point of	No intake question addresses this point of focus; manage-	--	Priya Raman, Chief	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
	(Internal)	focus.	ment's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.		Technology Officer	
CC3.1M	Reflects Entity Activities (Internal)	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1N	Reflects External Laws and Regulations	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1O	Considers Tolerances for Risk (Compliance)	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.1 (E1) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.1P	Establishes Sub-Objectives for Risk Assessment	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.						
CC3.2A	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.2 (E1, E2) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open; the evidence request for risk register is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.2B	Analyzes Internal and External Factors	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC3.2C	Involves Appropriate Levels of Management	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC3.2D	Estimates Significance of Risks Identified	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC3.2E	Determines How to Respond to Risks	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC3.2F	Identifies Threats to Objectives	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC3.2G	Identifies Vulnerabilities of System Components and Third Parties	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC3.2H	Assesses the Significance of the Risks	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.						
CC3.3A	Considers Various Types of Fraud	Not in place per management: fraud and insider misuse in the risk assessment (F-10 in Section 2.1).	Management answered No to fraud and insider misuse in the risk assessment; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC3.3B	Assesses Incentives and Pressures	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.3 (E1, E4) do not address this point of focus; the remediation items for formal risk assessment in the last 12 months and fraud and insider misuse in the risk assessment are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.3C	Assesses Opportunities	Not in place per management: fraud and insider misuse in the risk assessment (F-10 in Section 2.1).	Management answered No to fraud and insider misuse in the risk assessment; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC3.3D	Assesses Attitudes and Rationalizations	Not in place per management: fraud and insider misuse in the risk assessment (F-10 in Section 2.1).	Management answered No to fraud and insider misuse in the risk assessment; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC3.3E	Considers the Risks Related to the Use of IT and Access to Information	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1); fraud and insider misuse in the risk assessment (F-10 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open; management answered No to fraud and insider misuse in the risk assessment; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.						
CC3.4A	Assesses Changes in the External Environment	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.4 (E1, E5) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open; the evidence request for risk assessment of significant changes before rollout is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.4B	Assesses Changes in the Business Model	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.4 (E1, E5) do not address this point of focus; the remediation item for formal risk assessment in the last 12 months is still open; the evidence request for risk assessment of significant changes before rollout is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC3.4C	Assesses Changes in Leadership	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC3.4 (E1, E5) do not ad-	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			dress this point of focus; the remediation item for formal risk assessment in the last 12 months is still open; the evidence request for risk assessment of significant changes before rollout is still open.			
CC3.4D	Assess Changes in Systems and Technology	Significant changes are assessed for risk before rollout.	Management's answer on risk assessment of significant changes before rollout supports this point of focus; the remediation item for formal risk assessment in the last 12 months is still open; the evidence request for risk assessment of significant changes before rollout is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC3.4E	Assess Changes in Vendor and Business Partner Relationships	Significant changes are assessed for risk before rollout.	Management's answer on risk assessment of significant changes before rollout supports this point of focus; the remediation item for formal risk assessment in the last 12 months is still open; the evidence request for risk assessment of significant changes before rollout is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC3.4F	Assesses Changes in Threats and Vulnerabilities	Not in place per management: formal risk assessment in the last 12 months (F-08 in Section 2.1).	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC4: Monitoring Activities						
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Exception on this criterion as a whole: weekly review of administrator activity (F-29). See Section 2.1.						
CC4.1A	Considers a Mix of Ongoing and Separate Evaluations	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC4.1 (B8, C4, K1, K2, M3, R1) do not address this point of focus; 5 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC4.1B	Considers Rate of Change	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC4.1 (B8, C4, K1, K2, M3, R1) do not address this point of focus; 5 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC4.1C	Establishes Baseline Understanding	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC4.1 (B8, C4, K1, K2, M3, R1) do not address this point of focus; 5 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC4.1D	Uses Knowledgeable Personnel	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC4.1 (B8, C4, K1, K2, M3, R1) do not address this point of focus; 5 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC4.1E	Integrates With Business Processes	Application and infrastructure logs are collected centrally.	Management's answer on centralized log collection sup-	--	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			ports this point of focus; 5 evidence requests for this point of focus are still open; no policy or artifact is on file.			
CC4.1F	Adjusts Scope and Frequency	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC4.1 (B8, C4, K1, K2, M3, R1) do not address this point of focus; 5 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC4.1G	Objectively Evaluates	A body outside day to day management reviews security matters at least twice a year. A penetration test is performed annually. Management reviews the overall security and compliance program at least annually.	Management's answers on independent oversight of security, annual penetration test and annual management review of the security program support this point of focus; 5 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC4.1H	Considers Different Types of Ongoing and Separate Evaluations	A penetration test is performed annually.	Management's answer on annual penetration test supports this point of focus; 5 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.						
CC4.2A	Assesses Results	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC4.2 (K1, R2, R3, R4) do not address this point of focus; 3 evi-	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			dence requests for this point of focus are still open.			
CC4.2B	Communicates Deficiencies	Asked for any reporting of control deficiencies to management and who receives it, management answered "Anyone who finds a control deficiency files it in Linear with the security label; the security owner reviews the list weekly and reports open items to the CEO at the monthly leadership meeting."	Management described any reporting of control deficiencies to management and who receives it in writing (Appendix C); 3 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC4.2C	Monitors Corrective Action	There is a process to track and close remediation items from audits, incidents, tests or reviews.	Management's answer on tracking and closing remediation items supports this point of focus; 3 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC5: Control Activities						
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.						
CC5.1A	Integrates With Risk Assessment	Significant changes are assessed for risk before rollout.	Management's answer on risk assessment of significant changes before rollout supports this point of focus; the evidence request for risk assessment of significant changes before rollout is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC5.1B	Considers Entity-Specific Factors	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.1 (E5) do not address this point of focus; the evidence request for risk assessment	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			of significant changes before roll-out is still open.			
CC5.1C	Determines Relevant Business Processes	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.1 (E5) do not address this point of focus; the evidence request for risk assessment of significant changes before roll-out is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC5.1D	Evaluates a Mix of Control Activity Types	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.1 (E5) do not address this point of focus; the evidence request for risk assessment of significant changes before roll-out is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC5.1E	Considers at What Level Activities Are Applied	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.1 (E5) do not address this point of focus; the evidence request for risk assessment of significant changes before roll-out is still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC5.1F	Addresses Segregation of Duties	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.1 (E5) do not address this point of focus; the evidence request for risk assessment of significant changes before roll-out is still open.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.						
CC5.2A	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.2 (F6, M5) do not address this point of focus; the evidence requests for inventory of production systems and applications with owners and hardening or configuration baseline for production systems are still open.	--	Tom Iyer	Not assessed
CC5.2B	Establishes Relevant Technology Infrastructure Control Activities	A documented hardening or configuration baseline is applied to production systems.	Management's answer on hardening or configuration baseline for production systems supports this point of focus; the evidence requests for inventory of production systems and applications with owners and hardening or configuration baseline for production systems are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC5.2C	Establishes Relevant Security Management Process Controls Activities	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.2 (F6, M5) do not address this point of focus; the evidence requests for inventory of production systems and applications with owners and hardening or configuration baseline for production systems are still open.	--	Tom Iyer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC5.2D	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.2 (F6, M5) do not address this point of focus; the evidence requests for inventory of production systems and applications with owners and hardening or configuration baseline for production systems are still open.	--	Tom Iyer	Not assessed
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.						
CC5.3A	Establishes Policies and Procedures to Support Deployment of Management's Directives	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.3 (B2, R1, R2) do not address this point of focus; the evidence requests for annual management review of the security program and tracking and closing remediation items are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC5.3B	Establishes Responsibility and Accountability for Executing Policies and Procedures	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.3 (B2, R1, R2) do not address this point of focus; the evidence requests for annual management review of the security program and tracking and closing remediation items are still open.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC5.3C	Performs in a Timely Manner	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.3 (B2, R1, R2) do not address this point of focus; the evidence requests for annual management review of the security program and tracking and closing remediation items are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC5.3D	Takes Corrective Action	There is a process to track and close remediation items from audits, incidents, tests or reviews.	Management's answer on tracking and closing remediation items supports this point of focus; the evidence requests for annual management review of the security program and tracking and closing remediation items are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC5.3E	Performs Using Competent Personnel	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC5.3 (B2, R1, R2) do not address this point of focus; the evidence requests for annual management review of the security program and tracking and closing remediation items are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC5.3F	Reassesses Policies and Procedures	Management reviews the overall security and compliance program at least annually.	Management's answer on annual management review of the security program supports this point of focus; the evidence requests for annual management review of the security program and tracking and closing	--	Priya Raman, Chief Technology Officer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			remediation items are still open; no policy or artifact is on file.			
CC6: Logical and Physical Access Controls						
CC6.1. The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. Exception on this criterion as a whole: device management (MDM or EDR) (F-12). See Section 2.1.						
CC6.1A	Identifies and Manages the Inventory of Information Assets	An inventory of production systems, data stores and SaaS applications with an owner for each is maintained. A data classification scheme is applied with levels up to restricted or confidential data.	Management's answers on inventory of production systems and applications with owners and data classification scheme support this point of focus; 4 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.1B	Assesses New Architectures	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.1 (F1, F2, F3, F5, F6, G1 and 8 more) do not address this point of focus; 4 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC6.1C	Restricts Logical Access	Multi-factor authentication (MFA) is required for cloud console access. Role-based access is used for production systems.	Management's answers on multi-factor authentication for cloud console access and role-based access to production support this point of focus; 4 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.1D	Identifies and Authenticates Users	Multi-factor authentication (MFA) is required for cloud console access.	Management's answer on multi-factor authentication for cloud console access supports this point of focus; arti-	EVD-001	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			fact on file: EVD-001; 4 evidence requests for this point of focus are still open.			
CC6.1E	Consider Network Segmentation	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.1 (F1, F2, F3, F5, F6, G1 and 8 more) do not address this point of focus; 4 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC6.1F	Manages Points of Access	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.1 (F1, F2, F3, F5, F6, G1 and 8 more) do not address this point of focus; 4 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC6.1G	Restricts Access to Information Assets	A data classification scheme is applied with levels up to restricted or confidential data.	Management's answer on data classification scheme supports this point of focus; 4 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.1H	Manages Identification and Authentication	Multi-factor authentication (MFA) is required for cloud console access.	Management's answer on multi-factor authentication for cloud console access supports this point of focus; artifact on file: EVD-001; 4 evidence requests for this point of focus are still open.	EVD-001	Tom Iyer	Implemented per management
CC6.1I	Manages Credentials for Infrastructure and Software	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.1	--	Tom Iyer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			(F1, F2, F3, F5, F6, G1 and 8 more) do not address this point of focus; 4 evidence requests for this point of focus are still open.			
CC6.1J	Uses Encryption to Protect Data	Databases and backups are encrypted at rest.	Management's answer on encryption at rest for databases and backups supports this point of focus; 4 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.1K	Protects Cryptographic Keys	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.1 (F1, F2, F3, F5, F6, G1 and 8 more) do not address this point of focus; 4 evidence requests for this point of focus are still open.	--	Tom Iyer	Not assessed
CC6.2. Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.						
CC6.2A	Creates Access Credentials to Protected Information Assets	Not in place per management: manager approval before production access is granted (F-19 in Section 2.1).	Management answered No to manager approval before production access is granted; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC6.2B	Reviews Validity of Access Credentials	A documented review of all user access to production is performed annually.	Management's answer on periodic review of user access to production supports this point of focus only in part; 3 remediation items for this point of focus are still open; the evidence requests for role-based access to production and periodic review of user	--	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			access to production are still open; no policy or artifact is on file.			
CC6.2C	Prevents the Use of Credentials When No Longer Valid	Not in place per management: access removal within 24 hours of termination (F-17 in Section 2.1); offboarding checklist recording access revocation (F-23 in Section 2.1).	Management answered No to access removal within 24 hours of termination; its remediation item is still open; management answered No to offboarding checklist recording access revocation; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC6.3. The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.						
CC6.3A	Creates or Modifies Access to Protected Information Assets	Not in place per management: manager approval before production access is granted (F-19 in Section 2.1).	Management answered No to manager approval before production access is granted; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC6.3B	Removes Access to Protected Information Assets	Not in place per management: access removal within 24 hours of termination (F-17 in Section 2.1).	Management answered No to access removal within 24 hours of termination; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC6.3C	Uses Access Control Structures	Role-based access is used for production systems.	Management's answer on role-based access to production supports this point of focus; the remediation items for access removal within 24 hours of termination and manager approval before production access is granted are still open; the evidence requests for role-based access to production and periodic review of user access to production are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC6.3D	Reviews Access Roles and Rules	A documented review of all user access to production is performed annually.	Management's answer on periodic review of user access to production supports this point of focus only in part; the remediation items for access removal within 24 hours of termination and manager approval before production access is granted are still open; the evidence requests for role-based access to production and periodic review of user access to production are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.4. The entity restricts physical access to facilities and protected information assets to authorized personnel to meet the entity's objectives. Exception on this criterion as a whole: separation of production work areas from shared space (F-01). See Section 2.1.						
CC6.4A	Creates or Modifies Physical Access	Access to the offices or coworking spaces is controlled by a badge or electronic access control system. Visitors are escorted and recorded when entering areas with company systems or records.	Management's answers on physical access control to offices and visitor escort and logging support this point of focus; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC6.4B	Removes Physical Access	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.4 (A7a, A7b, A7c) do not address this point of focus.	--	Priya Raman, Chief Technology Officer	Not assessed
CC6.4C	Recovers Physical Devices	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.4 (A7a, A7b, A7c) do not address this point of focus.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC6.4D	Reviews Physical Access	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.4 (A7a, A7b, A7c) do not address this point of focus.	--	Priya Raman, Chief Technology Officer	Not assessed
CC6.5. The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.						
CC6.5A	Removes Data and Software for Disposal	Asked for any retention period and secure disposal method for customer data, management answered "Customer data is kept for the life of the contract plus 90 days, then deleted from the production database and from backups as they expire at 35 days. Laptops are wiped through device management before reissue."	Management described any retention period and secure disposal method for customer data in writing (Appendix C); the evidence request for any retention period and secure disposal method for customer data is still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.6. The entity implements logical access security measures to protect against threats from sources outside its system boundaries.						
CC6.6A	Restricts Access	A web application firewall (WAF) or equivalent is in place.	Management's answer on web application firewall supports this point of focus; the evidence request for web application firewall is still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.6B	Protects Identification and Authentication Credentials	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.6 (G1, L1, L2, L3) do not address this point of focus; the evidence request for web application firewall is still open.	--	Tom Iyer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC6.6C	Requires Additional Authentication or Credentials	Multi-factor authentication (MFA) is required for cloud console access.	Management's answer on multi-factor authentication for cloud console access supports this point of focus; artifact on file: EVD-001; the evidence request for web application firewall is still open.	EVD-001	Tom Iyer	Implemented per management
CC6.6D	Implements Boundary Protection Systems	A web application firewall (WAF) or equivalent is in place.	Management's answer on web application firewall supports this point of focus; the evidence request for web application firewall is still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.7. The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.						
CC6.7A	Restricts the Ability to Perform Transmission	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.7 (F2, I2, I4) do not address this point of focus; the evidence request for TLS on all external connections is still open.	--	Tom Iyer	Not assessed
CC6.7B	Uses Encryption Technologies or Secure Communication Channels to Protect Data	Transport Layer Security (TLS) is used for all external connections.	Management's answer on TLS on all external connections supports this point of focus; the evidence request for TLS on all external connections is still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.7C	Protects Removal Media	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.7 (F2, I2, I4) do not address this point of focus; the evidence	--	Tom Iyer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			request for TLS on all external connections is still open.			
CC6.7D	Protects Endpoint Devices	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.7 (F2, I2, I4) do not address this point of focus; the evidence request for TLS on all external connections is still open.	--	Tom Iyer	Not assessed
CC6.8. The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. Exception on this criterion as a whole: device management (MDM or EDR) (F-12). See Section 2.1.						
CC6.8A	Restricts Installation and Modification of Application and Software	Endpoint protection is installed and kept up to date on all company laptops.	Management's answer on endpoint protection on laptops supports this point of focus; the evidence request for endpoint protection on laptops is still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC6.8B	Detects Unauthorized Changes to Software and Configuration Parameters	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.8 (F3, F4) do not address this point of focus; the evidence request for endpoint protection on laptops is still open.	--	Tom Iyer	Not assessed
CC6.8C	Uses a Defined Change Control Process	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.8 (F3, F4) do not address this point of focus; the evidence request for endpoint protection on laptops is still open.	--	Tom Iyer	Not assessed
CC6.8D	Uses Antivirus and Anti-Malware	Endpoint protection is installed and kept up to date on all company	Management's answer on endpoint protection on laptops supports this	--	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
	Software	laptops.	point of focus; the evidence request for endpoint protection on laptops is still open; no policy or artifact is on file.			
CC6.8E	Scans Information Assets From Outside the Entity for Malware and Other Unauthorized Software	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC6.8 (F3, F4) do not address this point of focus; the evidence request for endpoint protection on laptops is still open.	--	Tom Iyer	Not assessed
CC7: System Operations						
CC7.1. To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.						
CC7.1A	Uses Defined Configuration Standards	A documented hardening or configuration baseline is applied to production systems.	Management's answer on hardening or configuration baseline for production systems supports this point of focus; the remediation item for monthly internal vulnerability scans is still open; 3 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC7.1B	Monitors Infrastructure and Software	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC7.1 (M1, M2, M3, M4, M5) do not address this point of focus; the remediation item for monthly internal vulnerability scans is still open; 3 evidence requests for this point of focus are still open.	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC7.1C	Implements Change-Detection Mechanisms	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC7.1 (M1, M2, M3, M4, M5) do not address this point of focus; the remediation item for monthly internal vulnerability scans is still open; 3 evidence requests for this point of focus are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC7.1D	Detects Unknown or Unauthorized Components	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC7.1 (M1, M2, M3, M4, M5) do not address this point of focus; the remediation item for monthly internal vulnerability scans is still open; 3 evidence requests for this point of focus are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC7.1E	Conducts Vulnerability Scans	Not in place per management: monthly internal vulnerability scans (F-32 in Section 2.1).	Management answered No to monthly internal vulnerability scans; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC7.2. The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Exception on this criterion as a whole: weekly review of administrator activity (F-29). See Section 2.1.						
CC7.2A	Implements Detection Policies, Procedures, and Tools	Application and infrastructure logs are collected centrally.	Management's answer on centralized log collection supports this point of focus; the evidence requests for centralized log collection and alerting for security events are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC7.2B	Designs Detection Measures	Alerting is configured for security events.	Management's answer on alerting for security events supports this point of focus; the evidence requests for centralized log collection and alerting for security events are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC7.3. The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.						
CC7.3A	Responds to Security Incidents	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC7.3B	Communicates and Reviews Detected Security Events	Alerting is configured for security events.	Management's answer on alerting for security events supports this point of focus; the remediation item for approved incident response plan is still open; the evidence request for alerting for security events is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC7.3C	Develops and Implements Procedures to Analyze Security Incidents	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC7.4. The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.						
CC7.4A	Assigns Roles and Responsibilities	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC7.4B	Contains and Responds to Security Incidents	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC7.4C	Mitigates Ongoing Security Incidents	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC7.4D	Resolves Security Incidents	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC7.4E	Restores Operations	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	Exception - see Section 2.1
CC7.4K	Periodically Evaluates Incidents	Root cause analysis is performed for high-severity incidents.	Management's answer on root cause analysis for high-severity incidents supports this point of focus; the remediation item for approved incident response plan is still open; the evidence request for root cause analysis for high-severity incidents is still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC7.5. The entity identifies, develops, and implements activities to recover from identified security incidents. Exception on this criterion as a whole: multi-region or multi-zone recovery strategy (F-44). See Section 2.1.						
CC7.5A	Restores the Affected Environment	Not in place per management: approved incident response plan (F-41 in Section 2.1).	Management answered No to approved incident response plan; its remediation item is still open.	--	Tom Iyer	Exception - see Section 2.1
CC7.5B	Communicates Information About the	Not in place per management: approved incident response plan (F-	Management answered No to approved incident re-	--	Tom Iyer	Exception - see Section 2.1

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
	Incident	41 in Section 2.1).	sponse plan; its remediation item is still open.			
CC7.5C	Determines Root Cause of the Incident	Root cause analysis is performed for high-severity incidents.	Management's answer on root cause analysis for high-severity incidents supports this point of focus; the remediation items for approved incident response plan and annual disaster recovery test are still open; the evidence requests for backups of databases and volumes and root cause analysis for high-severity incidents are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC7.5D	Implements Changes to Prevent and Detect Recurrences	Root cause analysis is performed for high-severity incidents.	Management's answer on root cause analysis for high-severity incidents supports this point of focus; the remediation items for approved incident response plan and annual disaster recovery test are still open; the evidence requests for backups of databases and volumes and root cause analysis for high-severity incidents are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC7.5E	Improves Response and Recovery Procedures	Root cause analysis is performed for high-severity incidents.	Management's answer on root cause analysis for high-severity incidents supports this point of focus; the remediation items for approved incident response plan and annual disaster recovery test are still open; the evidence	--	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			requests for backups of databases and volumes and root cause analysis for high-severity incidents are still open; no policy or artifact is on file.			
CC7.5F	Implements Incident Recovery Plan Testing	Not in place per management: annual disaster recovery test (F-45 in Section 2.1).	Management answered No to annual disaster recovery test; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC8: Change Management						
CC8.1. The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.						
CC8.1A	Manages Changes Throughout the System Life Cycle	Changes are tracked in a ticket or pull request system.	Management's answer on change tracking in tickets or pull requests supports this point of focus; artifact on file: EVD-002; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.	EVD-002	Tom Iyer	Implemented per management
CC8.1B	Authorizes Changes	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC8.1 (N1, N2, N3, N4, N5) do not address this point of focus; the remediation items for deployment approval by someone other than the author and documented emergency	--	Tom Iyer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.			
CC8.1C	Designs and Develops Changes	Development, test, and production environments are separated.	Management's answer on separation of development, test and production environments supports this point of focus; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open; no policy or artifact is on file.	--	Tom Iyer	Implemented per management
CC8.1D	Documents Changes	Changes are tracked in a ticket or pull request system.	Management's answer on change tracking in tickets or pull requests supports this point of focus; artifact on file: EVD-002; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.	EVD-002	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC8.1E	Tracks System Changes	Changes are tracked in a ticket or pull request system.	Management's answer on change tracking in tickets or pull requests supports this point of focus; artifact on file: EVD-002; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.	EVD-002	Tom Iyer	Implemented per management
CC8.1F	Configures Software	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC8.1 (N1, N2, N3, N4, N5) do not address this point of focus; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.	--	Tom Iyer	Not assessed
CC8.1G	Tests System Changes	Peer review is required before deployment. Development, test, and production environments are separated.	Management's answers on peer review before deployment and separation of development, test and production environments support this point of focus; the remediation items for deploy-	--	Tom Iyer	Implemented per management

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			ment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open; no policy or artifact is on file.			
CC8.1H	Approves System Changes	Not in place per management: deployment approval by someone other than the author (F-40 in Section 2.1).	Management answered No to deployment approval by someone other than the author; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC8.1I	Deploys System Changes	Not in place per management: deployment approval by someone other than the author (F-40 in Section 2.1).	Management answered No to deployment approval by someone other than the author; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC8.1J	Identifies and Evaluates System Changes	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC8.1 (N1, N2, N3, N4, N5) do not address this point of focus; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.	--	Tom Iyer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
CC8.1K	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC8.1 (N1, N2, N3, N4, N5) do not address this point of focus; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.	--	Tom Iyer	Not assessed
CC8.1L	Creates Baseline Configuration of IT Technology	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC8.1 (N1, N2, N3, N4, N5) do not address this point of focus; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.	--	Tom Iyer	Not assessed
CC8.1M	Provides for Changes Necessary in Emergency Situations	Not in place per management: documented emergency change procedure (F-39 in Section 2.1).	Management answered No to documented emergency change procedure; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC8.1N	Manages Patch Changes	Not addressed at intake: no intake question addresses this point of	No intake question addresses this point of focus; manage-	--	Tom Iyer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
		focus.	ment's intake answers under CC8.1 (N1, N2, N3, N4, N5) do not address this point of focus; the remediation items for deployment approval by someone other than the author and documented emergency change procedure are still open; the evidence requests for peer review before deployment and separation of development, test and production environments are still open.			
CC9: Risk Mitigation						
CC9.1. The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Exception on this criterion as a whole: multi-region or multi-zone recovery strategy (F-44). See Section 2.1.						
CC9.1A	Considers Mitigation of Risks of Business Disruption	Not in place per management: annual disaster recovery test (F-45 in Section 2.1).	Management answered No to annual disaster recovery test; its remediation item is still open.	--	Tom Iyer	**Exception - see Section 2.1**
CC9.1B	Consider the Use of Insurance to Mitigate Financial Impact Risks	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC9.1 (P1, P4, P5) do not address this point of focus; the remediation item for annual disaster recovery test is still open; the evidence request for backups of databases and volumes is still open.	--	Tom Iyer	Not assessed
CC9.2. The entity assesses and manages risks associated with vendors and business partners.						
CC9.2A	Establishes Requirements for Vendor and Business Partner Engagements	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC9.2 (C3, C4, F6, Q1, Q3)	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			do not address this point of focus; the remediation item for vendor risk reviews before onboarding and yearly is still open; 4 evidence requests for this point of focus are still open.			
CC9.2B	Identifies Vulnerabilities	Not in place per management: vendor risk reviews before onboarding and yearly (F-46 in Section 2.1).	Management answered No to vendor risk reviews before onboarding and yearly; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC9.2C	Assesses Vendor and Business Partner Risks	Not in place per management: vendor risk reviews before onboarding and yearly (F-46 in Section 2.1).	Management answered No to vendor risk reviews before onboarding and yearly; its remediation item is still open.	--	Priya Raman, Chief Technology Officer	**Exception - see Section 2.1**
CC9.2D	Assigns Responsibility and Accountability for Managing Vendors and Business Partners	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC9.2 (C3, C4, F6, Q1, Q3) do not address this point of focus; the remediation item for vendor risk reviews before onboarding and yearly is still open; 4 evidence requests for this point of focus are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC9.2E	Establishes Communication Protocols for Vendors and Business Partners	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC9.2 (C3, C4, F6, Q1, Q3) do not address this point of focus; the remediation item for vendor risk reviews before onboarding and yearly is still open; 4 evidence re-	--	Priya Raman, Chief Technology Officer	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
			quests for this point of focus are still open.			
CC9.2F	Establishes Exception Handling Procedures From Vendors and Business Partners	Not addressed at intake: no intake question addresses this point of focus.	No intake question addresses this point of focus; management's intake answers under CC9.2 (C3, C4, F6, Q1, Q3) do not address this point of focus; the remediation item for vendor risk reviews before onboarding and yearly is still open; 4 evidence requests for this point of focus are still open.	--	Priya Raman, Chief Technology Officer	Not assessed
CC9.2G	Assesses Vendor and Business Partner Performance	Asked for any vendors with production data access and the criticality and last review date of each, management answered "Amazon Web Services (hosting), Okta (identity), GitHub (source control), Datadog (monitoring), Stripe (payments), Linear (change tracking)".	Management described any vendors with production data access and the criticality and last review date of each in writing (Appendix C); the remediation item for vendor risk reviews before onboarding and yearly is still open; 4 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC9.2H	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments	The SOC 2 report or security attestation of each subservice organization is reviewed annually.	Management's answer on annual review of each subservice organization report supports this point of focus; the remediation item for vendor risk reviews before onboarding and yearly is still open; 4 evidence requests for this point of focus are still open; no policy or artifact is on file.	--	Priya Raman, Chief Technology Officer	Implemented per management
CC9.2I	Implements Procedures for Terminating	Not addressed at intake: no intake question addresses this point of	No intake question addresses this point of focus; manage-	--	Priya Raman, Chief	Not assessed

SAMPLE

TSC REF	COMMON CRITERIA / POINTS OF FOCUS	DESIGN OF CONTROLS	BASIS FOR STATUS	EVIDENCE	OWNER	MANAGEMENT STATUS
	Vendor and Business Partner Relationships	focus.	ment's intake answers under CC9.2 (C3, C4, F6, Q1, Q3) do not address this point of focus; the remediation item for vendor risk reviews before onboarding and yearly is still open; 4 evidence requests for this point of focus are still open.		Technology Officer	

SAMPLE

5. Disclosed Deviations and Deficiencies

Design deficiencies disclosed by management

21 of 33 in-scope control points carry an exception from the intake or remediation record as of 31 March 2026. Section 4 marks the points of focus each exception concerns; the findings referenced here are listed in Section 2.1 and scheduled in Appendix B.

CONTROL	CRITERION	MANAGEMENT'S DISCLOSURE	BASIS	FINDINGS	OWNER
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Not in place per management: security awareness training at hire and annually; offboarding checklist recording access revocation.	Management answered No to security awareness training at hire and annually; its remediation item is still open; management answered No to offboarding checklist recording access revocation; its remediation item is still open.	F-20, F-21, F-22, F-23	Priya Raman, Chief Technology Officer
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Not in place per management: security awareness training at hire and annually.	Management answered No to security awareness training at hire and annually; its remediation item is still open.	F-02, F-22	Priya Raman, Chief Technology Officer
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Not in place per management: communication of complementary user entity controls.	Management answered No to communication of complementary user entity controls; its remediation item is still open.	F-47	Priya Raman, Chief Technology Officer
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Not in place per management: formal risk assessment in the last 12 months.	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	F-08	Priya Raman, Chief Technology Officer

SAMPLE

CONTROL	CRITERION	MANAGEMENT'S DISCLOSURE	BASIS	FINDINGS	OWNER
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Not in place per management: formal risk assessment in the last 12 months.	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	F-08, F-09	Priya Raman, Chief Technology Officer
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Not in place per management: formal risk assessment in the last 12 months; fraud and insider misuse in the risk assessment.	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open; management answered No to fraud and insider misuse in the risk assessment; its remediation item is still open.	F-08, F-10	Priya Raman, Chief Technology Officer
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Not in place per management: formal risk assessment in the last 12 months.	Management answered No to formal risk assessment in the last 12 months; its remediation item is still open.	F-08, F-11	Priya Raman, Chief Technology Officer
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Not in place per management: weekly review of administrator activity.	Management answered No to weekly review of administrator activity; no remediation item covers it.	F-04, F-07, F-28, F-29, F-33, F-49	Tom Iyer

SAMPLE

CONTROL	CRITERION	MANAGEMENT'S DISCLOSURE	BASIS	FINDINGS	OWNER
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Not in place per management: device management (MDM or EDR).	Management answered No to device management (MDM or EDR); no remediation item covers it; artifact on file: EVD-001.	F-12, F-14, F-15, F-16, F-24, F-26	Tom Iyer
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Not in place per management: access removal within 24 hours of termination; manager approval before production access is granted; offboarding checklist recording access revocation.	Management answered No to access removal within 24 hours of termination; its remediation item is still open; management answered No to manager approval before production access is granted; its remediation item is still open; management answered No to offboarding checklist recording access revocation; its remediation item is still open.	F-16, F-17, F-18, F-19, F-23	Tom Iyer
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Not in place per management: access removal within 24 hours of termination; manager approval before production access is granted.	Management answered No to access removal within 24 hours of termination; its remediation item is still open; management answered No to manager approval before production access is granted; its remediation item is still open.	F-16, F-17, F-18, F-19	Tom Iyer

SAMPLE

CONTROL	CRITERION	MANAGEMENT'S DISCLOSURE	BASIS	FINDINGS	OWNER
CC6.4	The entity restricts physical access to facilities and protected information assets to authorized personnel to meet the entity's objectives.	Not in place per management: separation of production work areas from shared space.	Management answered No to separation of production work areas from shared space; no remediation item covers it.	F-01	Priya Raman, Chief Technology Officer
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Not in place per management: device management (MDM or EDR).	Management answered No to device management (MDM or EDR); no remediation item covers it.	F-12, F-13	Tom Iyer
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Not in place per management: monthly internal vulnerability scans.	Management answered No to monthly internal vulnerability scans; its remediation item is still open.	F-32, F-33, F-34, F-35	Priya Raman, Chief Technology Officer
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Not in place per management: weekly review of administrator activity.	Management answered No to weekly review of administrator activity; no remediation item covers it.	F-28, F-29, F-30	Tom Iyer

SAMPLE

CONTROL	CRITERION	MANAGEMENT'S DISCLOSURE	BASIS	FINDINGS	OWNER
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Not in place per management: approved incident response plan.	Management answered No to approved incident response plan; its remediation item is still open.	F-30, F-41	Priya Raman, Chief Technology Officer
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Not in place per management: approved incident response plan.	Management answered No to approved incident response plan; its remediation item is still open.	F-41, F-42	Priya Raman, Chief Technology Officer
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Not in place per management: approved incident response plan; multi-region or multi-zone recovery strategy; annual disaster recovery test.	Management answered No to approved incident response plan; its remediation item is still open; management answered No to multi-region or multi-zone recovery strategy; no remediation item covers it; management answered No to annual disaster recovery test; its remediation item is still open.	F-41, F-42, F-43, F-44, F-45	Tom Iyer

SAMPLE

CONTROL	CRITERION	MANAGEMENT'S DISCLOSURE	BASIS	FINDINGS	OWNER
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Not in place per management: documented emergency change procedure; deployment approval by someone other than the author.	Management answered No to documented emergency change procedure; its remediation item is still open; management answered No to deployment approval by someone other than the author; its remediation item is still open; artifact on file: EVD-002.	F-36, F-37, F-38, F-39, F-40	Tom Iyer
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Not in place per management: multi-region or multi-zone recovery strategy; annual disaster recovery test.	Management answered No to multi-region or multi-zone recovery strategy; no remediation item covers it; management answered No to annual disaster recovery test; its remediation item is still open.	F-43, F-44, F-45	Tom Iyer
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Not in place per management: vendor risk reviews before onboarding and yearly.	Management answered No to vendor risk reviews before onboarding and yearly; its remediation item is still open.	F-06, F-07, F-14, F-46, F-48	Priya Raman, Chief Technology Officer

SAMPLE

Appendix A. Evidence Cross-Reference

Every artifact on file for this assessment, identified by the same EVD reference the evidence binder and the auditor workspace use. Hashes are the first 16 hexadecimal characters of the SHA-256 recorded at upload; upload times are UTC as recorded. An artifact with no recorded hash or upload time is shown as such.

A.1 Evidence by control point

CONTROL	EVD	FILE NAME	TYPE	SHA-256 (FIRST 16)	UPLOADED	SOURCE
CC6.1	EVD-001	okta-mfa-policy.png	Text attestation	`not recorded`	1 February 2026 at 00:00 UTC	Upload
CC6.6	EVD-001	okta-mfa-policy.png	Text attestation	`not recorded`	1 February 2026 at 00:00 UTC	Upload
CC8.1	EVD-002	branch-protection.json	Text attestation	`not recorded`	3 February 2026 at 00:00 UTC	Integration

A.2 Evidence register (EVD to control points)

EVD	FILE NAME AND TITLE	TYPE	CONTROL POINTS
EVD-001	okta-mfa-policy.png Okta MFA enforcement policy	Text attestation	CC6.1, CC6.6
EVD-002	branch-protection.json GitHub branch protection settings	Text attestation	CC8.1

SAMPLE

Appendix B. Management Remediation Roadmap

49 open remediation items as of 31 March 2026. Target dates are the dates management recorded against each remediation item; an item with no recorded date is shown as not yet scheduled.

REF	ITEM	CRITERIA	OWNER	TARGET DATE	STATUS
F-01	Work areas with production access are not separated from public or shared space. Move production access to a separated work area or restrict production access to managed devices with screen privacy controls.	CC6.4	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-02	Supporting artifact not yet provided for documented security roles and responsibilities. Upload a supporting artifact for documented security roles and responsibilities.	CC1.3, CC2.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-03	Supporting artifact not yet provided for code of conduct acknowledgment. Upload a supporting artifact for code of conduct acknowledgment.	CC1.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-04	Supporting artifact not yet provided for independent oversight of security. Upload a supporting artifact for independent oversight of security.	CC1.2, CC4.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-05	Supporting artifact not yet provided for security responsibilities in performance expectations. Upload a supporting artifact for security responsibilities in performance expectations.	CC1.5	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-06	Supporting artifact not yet provided for SOC reports or risk questionnaires for subservice organizations. Upload a supporting artifact for SOC reports or risk questionnaires for subservice organizations.	CC9.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-07	Supporting artifact not yet provided for annual review of each subservice organization report. Upload a supporting artifact for annual review of each subservice organization report.	CC9.2, CC4.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-08	No formal information security risk assessment has been completed in the last 12 months. Perform and document a formal risk assessment covering the in-scope system, with an owner for each identified risk.	CC3.1, CC3.2, CC3.3, CC3.4	Priya Raman, Chief Technology Officer	Not yet scheduled	Open

SAMPLE

REF	ITEM	CRITERIA	OWNER	TARGET DATE	STATUS
F-09	Supporting artifact not yet provided for risk register. Upload a supporting artifact for risk register.	CC3.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-10	No risk assessment explicitly considers fraud and insider misuse (see F-08). Add fraud and insider misuse scenarios to the risk assessment, each with an owner and a mitigation.	CC3.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-11	Supporting artifact not yet provided for risk assessment of significant changes before rollout. Upload a supporting artifact for risk assessment of significant changes before rollout.	CC3.4, CC5.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-12	No device management tool (mobile device management or endpoint detection and response) is used for company laptops. Deploy a device management tool to every company laptop and enforce the baseline configuration through it.	CC6.8, CC6.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-13	Supporting artifact not yet provided for endpoint protection on laptops. Upload a supporting artifact for endpoint protection on laptops.	CC6.8	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-14	Supporting artifact not yet provided for inventory of production systems and applications with owners. Upload a supporting artifact for inventory of production systems and applications with owners.	CC6.1, CC5.2, CC9.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-16	Supporting artifact not yet provided for role-based access to production. Upload a supporting artifact for role-based access to production.	CC6.1, CC6.2, CC6.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-17	User access is not removed within 24 hours of termination. Add a 24 hour access removal step to the off-boarding checklist and retain the completed checklist for each departure.	CC6.2, CC6.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-18	Supporting artifact not yet provided for periodic review of user access to production. Upload a supporting artifact for periodic review of user access to production.	CC6.2, CC6.3, CC1.5	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-19	Access to production is not approved by a named manager before it is granted. Require a named manager to approve each production access request and retain the approval record.	CC6.2, CC6.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open

SAMPLE

REF	ITEM	CRITERIA	OWNER	TARGET DATE	STATUS
F-20	Supporting artifact not yet provided for background checks before start. Upload a supporting artifact for background checks before start.	CC1.4	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-21	Supporting artifact not yet provided for non-disclosure agreement at hire. Upload a supporting artifact for non-disclosure agreement at hire.	CC1.1, CC1.4	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-22	Security awareness training is not completed both at hire and annually. Assign security awareness training at hire and annually, and retain the completion record.	CC1.4, CC2.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-23	No documented offboarding checklist records access revocation for each departure. Adopt an offboarding checklist that records every access revocation, and retain the completed checklist for each departure.	CC6.2, CC1.4	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-24	Supporting artifact not yet provided for data classification scheme. Upload a supporting artifact for data classification scheme.	CC6.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-25	Supporting artifact not yet provided for TLS on all external connections. Upload a supporting artifact for TLS on all external connections.	CC6.7	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-26	Supporting artifact not yet provided for encryption at rest for databases and backups. Upload a supporting artifact for encryption at rest for databases and backups.	CC6.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-27	No supporting artifact is on file for management's answer about any retention period and secure disposal method for customer data. Upload a supporting artifact for management's answer about any retention period and secure disposal method for customer data.	CC6.5	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-28	Supporting artifact not yet provided for centralized log collection. Upload a supporting artifact for centralized log collection.	CC4.1, CC4.2, CC7.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-29	Administrator and operator activity is not both logged and reviewed weekly. Schedule a weekly review of administrator activity logs and retain the review record.	CC4.1, CC7.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open

SAMPLE

REF	ITEM	CRITERIA	OWNER	TARGET DATE	STATUS
F-30	Supporting artifact not yet provided for alerting for security events. Upload a supporting artifact for alerting for security events.	CC7.2, CC7.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-31	Supporting artifact not yet provided for web application firewall. Upload a supporting artifact for web application firewall.	CC6.6	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-32	Internal vulnerability scans do not run monthly. Schedule monthly internal vulnerability scans and retain the scan summary.	CC7.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-33	Supporting artifact not yet provided for annual penetration test. Upload a supporting artifact for annual penetration test.	CC7.1, CC4.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-34	Supporting artifact not yet provided for critical patch service level. Upload a supporting artifact for critical patch service level.	CC7.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-35	Supporting artifact not yet provided for hardening or configuration baseline for production systems. Upload a supporting artifact for hardening or configuration baseline for production systems.	CC7.1, CC5.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-37	Supporting artifact not yet provided for peer review before deployment. Upload a supporting artifact for peer review before deployment.	CC8.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-38	Supporting artifact not yet provided for separation of development, test and production environments. Upload a supporting artifact for separation of development, test and production environments.	CC8.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-39	No emergency change procedure is documented. Document an emergency change procedure with approval and post-change review steps in the secure development policy.	CC8.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-40	Production deployments are not approved by someone other than the author. Require approval from someone other than the author before a deployment reaches production, and export a sample of those approvals.	CC8.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open

SAMPLE

REF	ITEM	CRITERIA	OWNER	TARGET DATE	STATUS
F-41	No approved incident response plan exists. Approve an incident response plan with roles, severity levels, and escalation paths.	CC7.3, CC7.4, CC7.5	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-42	Supporting artifact not yet provided for root cause analysis for high-severity incidents. Upload a supporting artifact for root cause analysis for high-severity incidents.	CC7.4, CC7.5	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-43	Supporting artifact not yet provided for backups of databases and volumes. Upload a supporting artifact for backups of databases and volumes.	CC7.5, CC9.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-44	No multi-region or multi-zone recovery strategy is in place. Define a recovery strategy across zones or regions and document the recovery objectives.	CC7.5, CC9.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-45	No disaster recovery or business continuity plan test is performed at least annually. Run a disaster recovery test at least annually and retain the test record and lessons learned.	CC7.5, CC9.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-46	Vendor risk reviews are not performed before onboarding and yearly. Review each vendor before onboarding and annually, and record the outcome in a vendor register.	CC9.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-47	Customers are not informed of their complementary user entity controls. Document the complementary user entity controls in service agreements, onboarding materials, or a trust portal, and distribute them to all user entities.	CC2.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-48	No supporting artifact is on file for management's answer about any vendors with production data access and the criticality and last review date of each. Upload a supporting artifact for management's answer about any vendors with production data access and the criticality and last review date of each.	CC9.2	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-49	Supporting artifact not yet provided for annual management review of the security program. Upload a supporting artifact for annual management review of the security program.	CC1.2, CC4.1, CC5.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open
F-50	Supporting artifact not yet provided for tracking and closing remediation items. Upload a supporting artifact for tracking and closing remediation items.	CC4.2, CC5.3	Priya Raman, Chief Technology Officer	Not yet scheduled	Open

SAMPLE

REF	ITEM	CRITERIA	OWNER	TARGET DATE	STATUS
F-51	No supporting artifact is on file for management's answer about any reporting of control deficiencies to management and who receives it. Upload a supporting artifact for management's answer about any reporting of control deficiencies to management and who receives it.	CC4.2, CC2.1	Priya Raman, Chief Technology Officer	Not yet scheduled	Open

SAMPLE

Appendix C. Traceability

Every intake question, the answer management gave, where that answer is used in this report, and the artifacts on file for the control points it evidences. Rows marked not answered were not reached at intake and are not asserted anywhere in this report.

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
A1	Legal company name.	Northwind Example Systems, Inc. (fictional)	Cover, Section 2, Section 3	none
A2	Product or system name in scope.	Northwind Analytics Platform	Cover, Section 2, Section 3	none
A3	Office location(s) in scope.	One office in Austin, Texas. The rest of the team works remotely across the United States.	Section 4 (CC6.4); Cover, Section 2, Section 3; Section 5	none
A4	Cloud provider used for production.	AWS	Section 4 (CC6.1, CC9.2); Cover, Section 2, Section 3; Section 5	EVD-001
A5	Trust Services Category: Security (auto-included).	Yes	Cover, Section 2, Section 3	none
A6	As-of date for the Type 1 opinion.	2026-03-31	Cover, Section 2, Section 3	none
A7	Do you have physical offices or coworking spaces storing systems, laptops, or records?	Yes	Section 4 (CC6.4); Cover, Section 2, Section 3; Section 5	none
A7a	How is access to these offices or coworking spaces controlled?	Badge or electronic access control system	Section 4 (CC6.4); Cover, Section 2, Section 3; Section 5	none
A7b	Are visitors required to be escorted and recorded when entering areas with company systems or records?	Yes	Section 4 (CC6.4); Cover, Section 2, Section 3; Section 5	none
A7c	Are work areas with access to production systems or sensitive data separated from public or shared spaces?	No	Section 4 (CC6.4); Cover, Section 2, Section 3; Section 2.1 (F-01); Appendix B (F-01); Section 5	none
A8	Confirm your team is fully remote and no physical office stores company systems or records.	No	Not used in this report	none
A9	When do you need your SOC 2?	3 to 6 months	Not used in this report	none
B1	Primary owner for security and compliance (name and title).	Priya Raman, Chief Technology Officer	Section 4 (CC1.3); Section 2, Section 3	none
B2	Has management formally approved the security and compliance program in the last 12 months?	Yes	Section 4 (CC1.1, CC1.2, CC5.3); Section 2, Section 3	none

SAMPLE

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
B3	Are security roles and responsibilities documented and communicated?	Yes	Section 4 (CC1.3, CC2.2); Section 2, Section 3; Section 2.1 (F-02); Appendix B (F-02); Section 5	none
B4	Do employees acknowledge a Code of Conduct?	Yes	Section 4 (CC1.1); Section 2, Section 3; Section 2.1 (F-03); Appendix B (F-03)	none
B5	Summarize the scope and ethical standards covered by your Code of Conduct.	Conflicts of interest, acceptable use of company systems, confidentiality of customer data, and the duty to report a suspected security or ethics concern.	Section 4 (CC1.1); Section 2, Section 3	none
B6	Whistleblower or ethics reporting channel (email, hotline, or anonymous form).	ethics@northwind.example	Section 4 (CC1.1, CC2.2); Section 2, Section 3; Section 5	none
B7	Management body responsible for reviewing Code of Conduct or ethics reports.	The advisory board, at its quarterly meeting.	Section 4 (CC1.2); Section 2, Section 3	none
B8	How often does a body outside day-to-day management (a board, an advisory board, or a named independent advisor) review security matters?	Quarterly	Section 4 (CC1.2, CC4.1); Section 2, Section 3; Section 2.1 (F-04); Appendix B (F-04); Section 5	none
B8a	Which body or advisor is it?	The Northwind advisory board	Section 2, Section 3	none
B9	Are security responsibilities included in performance expectations or job descriptions for staff with production access?	Yes	Section 4 (CC1.5); Section 2, Section 3; Section 2.1 (F-05); Appendix B (F-05)	none
C1	List hosting, identity, code repo, and collaboration vendors used in production.	Amazon Web Services, Okta, GitHub, Datadog, Stripe, Linear	Section 4 (CC9.2); Section 2 (carve-out), Section 3; Section 5	none
C2	Use the carve-out method for subservice organizations?	Yes	Section 4 (CC9.2); Section 2 (carve-out), Section 3; Section 5	none
C3	Can you provide SOC reports or complete our risk questionnaire for each subservice org?	Yes	Section 4 (CC9.2); Section 2 (carve-out), Section 3; Section 2.1 (F-06); Appendix B (F-06); Section 5	none
C4	Do you review the SOC 2 report or security attestation of each subservice organization annually?	Yes	Section 4 (CC9.2, CC4.1); Section 2 (carve-out), Section 3; Section 2.1 (F-07); Appendix B (F-07); Section 5	none

SAMPLE

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
D1	One-sentence mission for the product.	Give operations teams a dashboard they can trust without hiring a data team.	Section 3	none
D2	Short overview of services provided to customers.	Northwind ingests customer operational data, models it, and serves dashboards, scheduled reports and a query API to mid-market operations teams.	Section 3	none
D4	Boundaries: confirm only the listed products and locations are in scope.	Confirmed: Yes. Notes: Only the Northwind Analytics Platform and the Austin office are in scope.	Section 3	none
E1	Completed a formal information security risk assessment in the last 12 months?	No	Section 4 (CC3.1, CC3.2, CC3.3, CC3.4); Section 2.1 (risks), Section 3; Section 2.1 (F-08); Appendix B (F-08); Section 5	none
E2	Where do you track identified risks and mitigation actions?	Spreadsheet or document	Section 4 (CC3.2); Section 2.1 (risks), Section 3; Section 2.1 (F-09); Appendix B (F-09); Section 5	none
E3	List the top three risks that could impact your service commitments or system availability.	A prolonged AWS region outage. An ingestion pipeline fault that serves one customer another customer's data. Loss of the single engineer who owns the deployment path.	Section 4 (CC3.2); Section 2.1 (risks), Section 3; Section 5	none
E4	Does your risk assessment explicitly consider fraud and insider misuse?	No	Section 4 (CC3.3); Section 2.1 (risks), Section 3; Section 2.1 (F-10); Appendix B (F-10); Section 5	none
E5	Are significant changes (new systems, vendors, or headcount changes) assessed for risk before rollout?	Yes	Section 4 (CC3.4, CC5.1); Section 2.1 (risks), Section 3; Section 2.1 (F-11); Appendix B (F-11); Section 5	none
F1	Do you maintain an inventory of devices that access production data?	Yes	Section 4 (CC6.1); Section 5	EVD-001
F2	Are all company laptops configured with full disk encryption?	Yes	Section 4 (CC6.1, CC6.7); Section 5	EVD-001
F3	Do you use a device management tool (MDM/EDR) for company laptops?	No	Section 4 (CC6.8, CC6.1); Section 2.1 (F-12); Appendix B (F-12); Section 5	EVD-001

SAMPLE

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
F4	Do all company laptops have endpoint protection installed and kept up to date?	Yes	Section 4 (CC6.8); Section 2.1 (F-13); Appendix B (F-13); Section 5	none
F5	Are users required to lock their devices when unattended?	Yes	Section 4 (CC6.1); Section 5	EVD-001
F6	Do you maintain an inventory of production systems, data stores, and SaaS applications with an owner for each?	Yes	Section 4 (CC6.1, CC5.2, CC9.2); Section 2.1 (F-14); Appendix B (F-14); Section 5	EVD-001
G1	MFA required for cloud console access?	Yes	Section 4 (CC6.1, CC6.6); Section 2.1 (F-15); Section 5	EVD-001
G2	Password policy minimum length.	12+	Section 4 (CC6.1); Section 5	EVD-001
G2a	Where is your password and authentication policy actually enforced?	Okta	Section 4 (CC6.1); Section 3; Section 5	EVD-001
G3	SSO used for SaaS apps?	No	Section 4 (CC6.1, CC6.2); Section 3; Section 5	EVD-001
G4	Role-based access for production systems?	Yes	Section 4 (CC6.1, CC6.2, CC6.3); Section 2.1 (F-16); Appendix B (F-16); Section 5	EVD-001
G5	Number of privileged admins for production.	3	Section 4 (CC6.3); Section 3; Section 5	none
G6	Account sharing prohibited?	Yes	Section 4 (CC6.1); Section 5	EVD-001
G7	User access removed within 24 hours of termination?	No	Section 4 (CC6.2, CC6.3); Section 2.1 (F-17); Appendix B (F-17); Section 5	none
G8	How often is a documented review of all user access to production performed?	Annually	Section 4 (CC6.2, CC6.3, CC1.5); Section 2.1 (F-18); Appendix B (F-18); Section 5	none
G9	Is access to production approved by a named manager before it is granted?	No	Section 4 (CC6.2, CC6.3); Section 2.1 (F-19); Appendix B (F-19); Section 5	none
H1	Background checks completed before start?	Yes	Section 4 (CC1.4); Section 2.1 (F-20); Appendix B (F-20); Section 5	none
H2	NDA signed at hire?	Yes	Section 4 (CC1.1, CC1.4); Section 2.1 (F-21); Appendix B (F-21); Section 5	none

SAMPLE

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
H3	Security awareness training at hire and annually?	No	Section 4 (CC1.4, CC2.2); Section 2.1 (F-22); Appendix B (F-22); Section 5	none
H4	Do you follow a documented off-boarding checklist that records access revocation for each departure?	No	Section 4 (CC6.2, CC1.4); Section 2.1 (F-23); Appendix B (F-23); Section 5	none
I1	Highest data classification level you apply.	Confidential	Section 4 (CC6.1); Section 2.1 (F-24); Appendix B (F-24); Section 5	EVD-001
I2	TLS for all external connections?	Yes	Section 4 (CC6.7); Section 2.1 (F-25); Appendix B (F-25)	none
I3	Encryption at rest for databases and backups?	Yes	Section 4 (CC6.1); Section 2.1 (F-26); Appendix B (F-26); Section 5	EVD-001
I4	Removable media allowed?	No	Section 4 (CC6.7)	none
I5	If removable media is allowed, is it encrypted?	Not applicable (hidden by a prior answer)	Not used in this report	none
I6	Encryption standard for data at rest.	AES-256 (AWS KMS managed keys)	Section 4 (CC6.1); Section 3; Section 5	EVD-001
I7	Encryption standard for data in transit.	TLS 1.3	Section 4 (CC6.7); Section 3	none
I8	Secrets or key management system used for encryption keys.	AWS Key Management Service	Section 4 (CC6.1); Section 3; Section 5	EVD-001
I9	Key rotation frequency.	Annually	Section 4 (CC6.1); Section 5	EVD-001
I10	What is your retention period for customer data, and how is it securely disposed of at end of life?	Customer data is kept for the life of the contract plus 90 days, then deleted from the production database and from backups as they expire at 35 days. Laptops are wiped through device management before reissue.	Section 4 (CC6.5); Section 2.1 (F-27); Appendix B (F-27)	none
J1	Trust Services Category: Privacy (not included).	No	Section 4 (scope)	none
K1	Centralized log collection for app and infrastructure?	Yes	Section 4 (CC4.1, CC4.2, CC7.2); Section 2.1 (F-28); Appendix B (F-28); Section 5	none
K2	Admin/operator activity logged and reviewed weekly?	No	Section 4 (CC4.1, CC7.2); Section 2.1 (F-29); Appendix B (F-29); Section 5	none

SAMPLE

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
K3	Alerting configured for security events?	Yes	Section 4 (CC7.2, CC7.3); Section 2.1 (F-30); Appendix B (F-30); Section 5	none
K4	Capacity and uptime monitored?	Yes	Section 4 (CC7.2); Section 5	none
L1	WAF or equivalent in place?	Yes	Section 4 (CC6.6); Section 2.1 (F-31); Appendix B (F-31)	EVD-001
L2	Security groups or firewall rules restrict production ingress?	Yes	Section 4 (CC6.6)	EVD-001
L3	Direct SSH/console access limited to named admins?	Yes	Section 4 (CC6.1, CC6.6); Section 5	EVD-001
M1	Internal vulnerability scans run monthly?	No	Section 4 (CC7.1); Section 2.1 (F-32); Appendix B (F-32); Section 5	none
M2	External vulnerability scans run at least quarterly?	Yes	Section 4 (CC7.1); Section 5	none
M3	Penetration test performed annually?	Yes	Section 4 (CC7.1, CC4.1); Section 2.1 (F-33); Appendix B (F-33); Section 5	none
M4	Critical patches applied within 30 days?	Yes	Section 4 (CC7.1); Section 2.1 (F-34); Appendix B (F-34); Section 5	none
M5	Do you apply a documented hardening or configuration baseline to production systems?	Yes	Section 4 (CC7.1, CC5.2); Section 2.1 (F-35); Appendix B (F-35); Section 5	none
N1	Changes tracked in a ticket or PR system?	Yes	Section 4 (CC8.1); Section 2.1 (F-36); Section 5	EVD-002
N2	Peer review required before deploy?	Yes	Section 4 (CC8.1); Section 2.1 (F-37); Appendix B (F-37); Section 5	EVD-002
N3	Separate dev, test, and prod environments?	Yes	Section 4 (CC8.1); Section 2.1 (F-38); Appendix B (F-38); Section 5	EVD-002
N4	Emergency change procedure documented?	No	Section 4 (CC8.1); Section 2.1 (F-39); Appendix B (F-39); Section 5	EVD-002
N5	Are production deployments approved by someone other than the author?	No	Section 4 (CC8.1); Section 2.1 (F-40); Appendix B (F-40); Section 5	EVD-002

SAMPLE

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
O1	Incident Response Plan exists and is approved?	No	Section 4 (CC7.3, CC7.4, CC7.5); Section 2.1 (F-41); Appendix B (F-41); Section 5	none
O2	Security events logged with severity, date, and status?	Yes	Section 4 (CC7.2, CC7.3); Section 5	none
O3	Root cause analysis performed for high-severity incidents?	Yes	Section 4 (CC7.4, CC7.5); Section 2.1 (F-42); Appendix B (F-42); Section 5	none
P1	Databases and volumes backed up?	Yes	Section 4 (CC7.5, CC9.1); Section 2.1 (F-43); Appendix B (F-43); Section 5	none
P2	Backup frequency.	Daily differential plus weekly full	Section 4 (CC7.5); Section 3; Section 5	none
P3	Backups encrypted?	Yes	Section 4 (CC6.1, CC7.5); Section 5	EVD-001
P4	Multi-region or multi-zone recovery strategy?	No	Section 4 (CC7.5, CC9.1); Section 2.1 (F-44); Appendix B (F-44); Section 5	none
P5	DR/BCP tested at least annually?	No	Section 4 (CC7.5, CC9.1); Section 2.1 (F-45); Appendix B (F-45); Section 5	none
Q1	Vendor risk reviews performed before onboarding and yearly?	No	Section 4 (CC9.2); Section 2.1 (F-46); Appendix B (F-46); Section 5	none
Q2	Customers informed of their complementary user entity controls?	No	Section 4 (CC2.3); Section 2.1 (F-47); Appendix B (F-47); Section 5	none
Q3	List each vendor with production data access, its criticality, and the date of its last review.	Amazon Web Services (hosting), Okta (identity), GitHub (source control), Datadog (monitoring), Stripe (payments), Linear (change tracking)	Section 4 (CC9.2); Section 2.1 (F-48); Appendix B (F-48); Section 5	none
R1	Does management review the overall security and compliance program at least annually?	Yes	Section 4 (CC1.2, CC4.1, CC5.3); Section 2.1 (F-49); Appendix B (F-49); Section 5	none
R2	Is there a process to track and close remediation items from audits, incidents, tests, or reviews?	Yes	Section 4 (CC4.2, CC5.3); Section 2.1 (F-50); Appendix B (F-50)	none
R3	Where are remediation items tracked?	Ticketing system	Section 4 (CC4.2)	none

SAMPLE

CODE	QUESTION	ANSWER	WHERE IT APPEARS	SUPPORTING EVD
R4	How are control deficiencies reported to management, and to whom?	Anyone who finds a control deficiency files it in Linear with the security label; the security owner reviews the list weekly and reports open items to the CEO at the monthly leadership meeting.	Section 4 (CC4.2, CC2.1); Section 2.1 (F-51); Appendix B (F-51)	none
S1	Single support email or portal for tickets (provide address/URL).	support@northwind.example	Section 4 (CC2.3); Section 3; Section 5	none
S2	Uptime SLA target (percentage or N/A).	99.9%	Section 4 (CC2.3); Section 3; Section 5	none
T1	Executive signatory name and title.	Marcus Webb, Chief Executive Officer	Section 2.1 (owner), Section 4 (owner)	none
T2	Security and compliance contact (name and email).	Priya Raman (priya.raman@northwind.example)	Section 2.1 (owner), Section 4 (owner)	none
T3	Technical contact (name and email).	Tom Iyer (tom.iyer@northwind.example)	Section 2.1 (owner), Section 4 (owner)	none
U1	Company overview (1-3 sentences describing what your company does).	Northwind Example Systems builds an analytics platform for mid-market operations teams. The company is fictional and exists only in this sample.	Section 3	none
U2	Approximate headcount (total employees and contractors).	18 employees and 3 contractors	Section 3	none
U3	Functional areas or departments (e.g., Engineering, Security, Operations, Support).	Engineering. Founders cover Security. Support.	Section 3	none

End of Report

Assembled by cybersoftware
Document ID: SOC2-RPT-SAMPLEREPORT | 28 September 2026
DRAFT. Not the issued report.
This document is confidential and intended solely for authorized parties.

SAMPLE