Control Environment Narrative

Sample Organization

Criteria satisfaction

Standard	Criteria Satisfied
TSC 2017	CC2.1, CC2.2, CC2.3, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3

Document history

Date	Comment
Jun 1 2018	Initial document

Contents

1 Control Environment Narrative

The following provides a description of the control structure of Sample Organization.

The intent of this description is to enumerate the logical, policy, and procedural controls that serve to monitor Sample Organization's application and data security. Changes uncovered by these procedures in the logical, policy, procedural, or customer environment are addressed by remediations specific to the noted change.

2 Logical Controls

Sample Organization employs several logical controls to protect confidential data and ensure normal operation of its core product.

- Mandatory data encryption at rest and in motion
- Multi-factor authentication for access to cloud infrastructure
- Activity and anomaly monitoring on production systems
- Vulnerability management program

3 Policy Controls

Sample Organization employs several policy controls to protect confidential data and ensure normal operation of its core product. These policies include, but are not limited to:

- Access Control Policy
- Encryption Policy
- Office Security Policy
- Password Policy
- Policy Training Policy
- Vendor Policy
- Workstation Policy

4 Procedural Controls

Sample Organization has numerous scheduled procedures to monitor and tune the effectiveness of ongoing security controls, and a series of event-driven procedures to respond to security-related events.

TODO: Finalize these lists

4.1 Scheduled Security and Audit Procedures

- Review Access [quarterly]
- Review Security Logs [weekly]
- Review Cyber Risk Assessment (enumerate possible compromise scenarios) [quarterly]
- Review Data Classification [quarterly]
- Backup Testing [quarterly]
- Disaster Recovery Testing [semi-annual]
- Review Devices & Workstations [quarterly]
- Review & Clear Low-Priority Alerts [weekly]
- Apply OS Patches [monthly]
- Verify Data Disposal per Retention Policy [quarterly]
- Conduct Security Training [annual]
- Review Security Monitoring and Alerting Configuration [quarterly]
- Penetration Test [annual]
- Whitebox Security Review [annual]
- SOC2 Audit [annual]

4.2 Event-Driven Security and Audit Procedures

- Onboard Employee
- Offboard Employee
- Investigate Security Alert
- Investigate Security Incident

5 Remediations

Sample Organization uses the outcomes of the aforementioned controls and procedures to identify shortcomings in the existing control environment. Once identified, these shortcomes are remediated by improving existing controls and procedures, and creating new controls and procedures as needed.

6 Communications

Sample Organization communicates relevant information regarding the functioning of the above controls with internal and external parties on an as-needed basis and according to statutory requirements.

6.1 Internal

Sample Organization communicates control outcomes, anomalies, and remediations internally using the following channels:

- Slack
- Email
- Github ticketing

6.2 External

Sample Organization communicates relevant control-related information to external parties including shareholders, customers, contractors, regulators, and government entities as needed according to contractual and regulatory/statutory obligation.