Security Architecture Narrative

XYZ Corporation

January 2019

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.6, CC6.7, CC7.1, CC7.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Security Architecture Narrative

Here we narrate why our org satisfies the control keys listed in the YML block

2 XYZ Corporation Product Architecture

Describe product architecture here, emphasizing security implications

3 XYZ Corporation Infrastructure

3.1 Product Infrastructure

Describe product infrastructure, emphasizing security measures

3.1.1 Authorized Personnel

- **AWS root account** access is granted only to the CTO and CEO
- **AWS IAM** access is granted to to a limited group of **Operators**
- **XYZ Corporation SSH** access is granted to a limited group of **Operators**
- **XYZ Corporation DB** access is granted to a limited group of **Data Operators**

3.2 IT Infrastructure

XYZ Corporation uses the following cloud services for its internal infrastructure:

- List cloud services

Access to these cloud services is limited according to the role of the XYZ Corporation employee and is reviewed quarterly as well as via regular onboarding/offboarding tasks for new and departing employees.

4 XYZ Corporation Workstations

XYZ Corporation workstations are hardened against logical and physical attack by the following measures:

- operating system must be within one generation of current
- full-disk encryption

- onboard antivirus/antimalware software
- OS and AV automatically updated

Workstation compliance with these measures is evaluated on a quarterly basis.

4.1 Remote Access

Many XYZ Corporation employees work remotely on a regular basis and connect to production and internal IT systems via the same methods as those employees connecting from the XYZ Corporation physical office, i.e., direct encrypted access to cloud services. It is the employee's responsibility to ensure that only authorized personnel use XYZ Corporation resources and access XYZ Corporation systems.

5 Access Review

Access to XYZ Corporation infrastructure, both internal and product, is reviewed quarterly and inactive users are removed. Any anomalies are reported to the security team for further investigation. When employees start or depart, an onboarding/offboarding procedure is followed to provision or deprovision appropriate account access.

6 Penetration Testing

XYZ Corporation commissions an external penetration test on an annual basis. All findings are immediately reviewed and addressed to the satisfaction of the CTO/CEO.

7 XYZ Corporation Physical Security

XYZ Corporation has one physical location, in San Francisco, CA. Key issuance is tracked by the Office Physical Security Policy Ledger. Office keys are additionally held by the lessor, property management, and custodial staff. These keys are not tracked by the Office Physical Security Policy Ledger. XYZ Corporation managers regularly review physical access privileges.

XYZ Corporation infrastructure is located within AWS. XYZ Corporation does not have physical access to AWS infrastructure.

8 Risk Assessment

XYZ Corporation updates its Cyber Risk Assessment on an annual basis in order to keep pace with the evolving threat landscape. The following is an inventory of adversarial and non-adversarial threats assessed to be of importance to XYZ Corporation.

8.1 Adversarial Threats

The following represents the inventory of adversarial threats:

Threat	Source	Vector	Target	Likelihood	Severity

8.2 Non-Adversarial Threats

The following represents the inventory of non-adversarial threats:

Threat	Vector	Target	Likelihood	Severity

9 References

9.1 Narratives

Products and Services Narrative System Architecture Narrative

9.2 Policies

Encryption Policy Log Management Policy Office Security Policy Remote Access Policy Security Incident Response Policy Workstation Policy

9.3 Procedures

Apply OS Patches Review & Clear Low-Priority Alerts Review Access Review Devices & Workstations