

Template

Version 1.0

Created by: Daniel Card

Service Cyber Security Architecture Review Template

# Abstract

This is a document template to help support organisations conduct a high-level security architecture review from a service perspective. It covers technical controls, processes, and provides a sample of documentation types to assess against. It is meant to be high level, it is designed to support learning and deconstruction of system security features, capabilities, and controls. It should be adapted and adopted as suitable for the context.

Contents

[Abstract 2](#_Toc121339292)

[Document Control 4](#_Toc121339293)

[Version Control 4](#_Toc121339294)

[Terms and Conditions 4](#_Toc121339295)

[Distribution 4](#_Toc121339296)

[Supplier 4](#_Toc121339297)

[Customer/Audience 4](#_Toc121339298)

[Service Overview 5](#_Toc121339299)

[Service Description of Business Context 6](#_Toc121339300)

[Service Controls 7](#_Toc121339301)

[Service Processes 9](#_Toc121339302)

[Service Documentation 10](#_Toc121339303)

[Data Sensitivity 11](#_Toc121339304)

[Data Locality 11](#_Toc121339305)

[Service Notes 12](#_Toc121339306)

# Document Control

|  |  |
| --- | --- |
| Title |  |
| Document Reference |  |
| Version |  |
| Author |  |
| Classification |  |
| Reviewer |  |
| Review Date |  |

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 0.1 | 07/12/2012 | Daniel Card | Initial creation |
| 1.0 | 07/12/2012 | Daniel Card | First Public Release |
|  |  |  |  |
|  |  |  |  |

# Terms and Conditions

This document template is the property of Xservus Limited. It has been produced to help support people developing a greater understanding of their technology and service security architecture. It may be used/modified with attribution to Xservus Limited.

# Distribution

## Supplier

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Job Title | Role | Email |
|  |  |  |  |

## Customer/Audience

|  |  |
| --- | --- |
| Name | Job Title |
|  |  |
|  |  |
|  |  |

# Service Overview

|  |  |
| --- | --- |
| Service Name |  |
| Service Status (Live/Test/Dev) |  |
| Service Operating Organisation Name |  |
| Service Description |  |
| Service Classification (Top Secret/Secret/Official Sensitive /Official) |  |
| Service Owner/Product Owner |  |
| Service Lead Architect |  |
| Service Lead Security Architect |  |
| Service Operations Manager |  |
| Service Change Manager |  |
| Service Incident Response Manager/Contact |  |
| Service Recovery Manager/Contact |  |
| Service Initial Online Date (Approx.) |  |
| Service Lifecycle (Sunrise/Operate/Sunset) |  |
| Expected Service Retirement Date (Approx.) |  |
| Service Business Criticality (H/M/L) |  |
| Service Availability Impact Risk (H/M/L) |  |
| Service Confidentiality Impact Risk (H/M/L) |  |
| Service Integrity Impact Risk (H/M/L) |  |
| Date of Last Security Architecture Review |  |
| Date of Last Security Testing Exercise |  |
| Date of Last Incident Simulation/Drill |  |
| Service Hours of Operation (e.g., 247) |  |
| Service Days of Operation (e.g., Monday-Sunday) |  |
| Service Days of Operation (e.g., 365) |  |
| Service Accreditation (e.g., NCSC Authority to Operate) |  |
| Audit Requirements (e.g., PCI DSS) |  |
| Assurance Requirements (Cyber Essentials/CE+/ISO27001) |  |
| Service Uptime Requirements (e.g., 99.99%) |  |
| Service Recovery Time Objectives (RTO) |  |
| Service Recovery Point Objective (RPO) |  |

# Service Description of Business Context

The following provides a high-level summary of the nature and purpose of the service:

|  |
| --- |
|  |

# Service Controls

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Control | Suitable for Service Type (yes/no) | In Place | Quality | Risk Summary Level | Notes |
| Registrar MFA |  |  |  |  |  |
| Public DNS MFA |  |  |  |  |  |
| Layer 3 DoS Protection on Ingress Interfaces |  |  |  |  |  |
| Web Application Firewall (WAF) on Ingress Interfaces |  |  |  |  |  |
| WAF Monitoring |  |  |  |  |  |
| WAF Altering |  |  |  |  |  |
| Ingress Perimeter Network Firewall |  |  |  |  |  |
| Ingress IPS |  |  |  |  |  |
| Load Balancing |  |  |  |  |  |
| Reverse Proxy |  |  |  |  |  |
| Front End Web Services Services/Host Based Firewall or Policy Based Traffic ACLs |  |  |  |  |  |
| Front End Services Logging (HTTP Access) |  |  |  |  |  |
| Font End and Backend Segmentation |  |  |  |  |  |
| Web Application Encryption in Transit (TLS) |  |  |  |  |  |
| Web Application Authentication |  |  |  |  |  |
| Web Application Authorisation |  |  |  |  |  |
| Web Application HTTP Access Logging |  |  |  |  |  |
| Web Application HTTP Access Monitoring |  |  |  |  |  |
| Web Front End Storage Encryption (FDE) |  |  |  |  |  |
| Web Application Input Sanitisation |  |  |  |  |  |
| Web Application Output Sanitisation |  |  |  |  |  |
| Web Application Platform Secure Configuration |  |  |  |  |  |
| Web Application Antivirus/Antimalware |  |  |  |  |  |
| Web Application Components (COTS) In Support and Patched |  |  |  |  |  |
| Backend Database Services Logging |  |  |  |  |  |
| Backend Database Services Monitoring |  |  |  |  |  |
| Backend Database Services Storage Antimalware |  |  |  |  |  |
| Cloud Services Authentication |  |  |  |  |  |
| Cloud Services MFA |  |  |  |  |  |
| Cloud Services Secure Configuration |  |  |  |  |  |
| Cloud Services Logging |  |  |  |  |  |
| Cloud Services Monitoring |  |  |  |  |  |
| Cloud Services Alerting |  |  |  |  |  |
| Protective DNS |  |  |  |  |  |
| Egress Web Content Filtering |  |  |  |  |  |
| Privileged Access Workstations/Servers |  |  |  |  |  |
| Secure Device Configuration |  |  |  |  |  |
| Secure Messaging (Email) Services |  |  |  |  |  |
| Secure Collaboration Services (DMS) |  |  |  |  |  |
| Secure Comms (e.g., Instant Messaging/Voice/Video) |  |  |  |  |  |
| Secure Password Management |  |  |  |  |  |
| Secure Key Management (KMS) |  |  |  |  |  |
| Secure CI/CD Platform |  |  |  |  |  |

# Service Processes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Process | Suitable for Service Type (yes/no) | In Place | Quality | Notes | Risk Summary Level |
| Asset Management |  |  |  |  |  |
| Identity & Access Management |  |  |  |  |  |
| Threat Intelligence |  |  |  |  |  |
| Breach Monitoring Process |  |  |  |  |  |
| Risk Management |  |  |  |  |  |
| Change Management |  |  |  |  |  |
| Configuration Management |  |  |  |  |  |
| Proactive Security Monitoring |  |  |  |  |  |
| Security Testing |  |  |  |  |  |
| Offensive Security Exercises |  |  |  |  |  |
| Incident Management |  |  |  |  |  |
| Crisis Response |  |  |  |  |  |
| CERT |  |  |  |  |  |
| Incident Response |  |  |  |  |  |
| Personnel Security |  |  |  |  |  |
| Supply Chain Security Assurance |  |  |  |  |  |
| Internal Audits |  |  |  |  |  |
| Backup & Recovery Management |  |  |  |  |  |
| Disaster Recovery Management |  |  |  |  |  |
| Business Continuity Management |  |  |  |  |  |

# Service Documentation

These are examples of common documentation sets that are useful to plan, design, build and operate a secure service, this is not exhaustive.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document | Suitable for Service Type (yes/no) | In Place | Quality | Notes | Risk Summary Level |
| Service Design |  |  |  |  |  |
| Service Security Policy |  |  |  |  |  |
| Service Security Management Plan |  |  |  |  |  |
| Service Operations Organisations Chart |  |  |  |  |  |
| Roles and Responsibilities |  |  |  |  |  |
| Service Level Agreement |  |  |  |  |  |
| Operational Level Agreement |  |  |  |  |  |
| Risk Appetite Statement |  |  |  |  |  |
| Risk Tolerance Statement |  |  |  |  |  |
| Risk Management Policy |  |  |  |  |  |
| Risk Management Process |  |  |  |  |  |
| Risk Management Procedures |  |  |  |  |  |
| Service Risk Register |  |  |  |  |  |
| Service Risk Treatment Plan |  |  |  |  |  |
| Service Asset Register |  |  |  |  |  |
| Service Configuration Documentation (per component/sub service) |  |  |  |  |  |
| layer 3 Service Network Topology |  |  |  |  |  |
| Layer 2 Service Topology |  |  |  |  |  |
| Software Bill of Materials |  |  |  |  |  |
| Security Standards |  |  |  |  |  |
| Security Control Descriptions |  |  |  |  |  |
| Data Flow Diagrams |  |  |  |  |  |
| Threat Models |  |  |  |  |  |
| Threat Intelligence Reports |  |  |  |  |  |
| Security Testing Reports (e.g., Pentest reports) |  |  |  |  |  |
| Authorised list of High Privileged Users |  |  |  |  |  |
| User Register |  |  |  |  |  |
| Supplier Register |  |  |  |  |  |

# Data Sensitivity

|  |  |
| --- | --- |
| Category | In Service |
| Credentials |  |
| Confidential Data (Organization) |  |
| Sensitive Data (Organisation) |  |
| Personal Identifiable Information (PII) |  |
| Financial Data |  |
| Card Holder Data |  |
| Third Part Confidential Data |  |

# Data Locality

|  |  |
| --- | --- |
| Category | Physical Location/Region |
| Credentials |  |
| Confidential Data (Organization) |  |
| Sensitive Data (Organisation) |  |
| Personal Identifiable Information (PII) |  |
| Financial Data |  |
| Card Holder Data |  |
| Third Part Confidential Data |  |

# Service Notes

Please provide any additional information that may be relevant to the service, it’s security and resilience.

|  |
| --- |
|  |