Title	ESA Controls Matrix
Author	Robert Campbell
Version	2.5 - Jan 2020
email	esa@assuredcontrol.com

Business Drivers and Requirements

Business Principles | Architecture Principles | Business Opportunities | Business Strategy | Business Requirements | Business Capability | Regulatory Compliance | Channels | Technology Strategy | Technology Capability | Technology Architecture

Security Drivers and Requirements

Situational Awareness | Industry Standards and Regulations | Principles | Policies, Standards and Guidelines | Security Patterns | Procedures | Compliance Audit | Enforcement | Contract Definition | Education and Awareness | Performance Metrics | Cyber Threats | Technology Threats | Business Threats | Security Testing Output

Security Controls

Network Security

Application Control | Content Security | Email Inspection and Control | Web Inspection and Control | Perimeter Defense | Data Centre Segregation | Firewall | IDS/IPS | UTM/Next Gen | Deep Packet Inspection | Geolocation | Network Time (NTP) | Network Access Control | Wireless | Application Control (App FW) | Pre Authentication (802.1x) | Guest Network | Encryption | Monitoring | Network Behaviour Analysis/Network Anomaly Detection | Network Forensics | Logging and Monitoring | Managed Services | Monitoring | Management | DDOS Protection | Network Encryption | Layer 2 encryption | Transport Layer Security | Virtual Private Networking | Out of Band Networking

Endpoint Security

Endpoint Defense | Anti Malware | Host Firewall | HIPS | Application White listing | Disk Encryption | Network Access Control | BYOD Security - Unified Endpoint Management | Remote Access/VPN | Secure Config Baselines | Build Compliance Checking | Logging and Monitoring | Process Protection | Sandboxing | Memory Protection

Physical Security

Physical Access Control | Security Passes - Identity | CCTV/Monitoring | Physical Asset Control | Cabinet Security

Web Services Security

Direct Authentication | Brokered Authentication | Data Confidentiality | Data Origin Authentication | Logging and Monitoring

Data Security

Database Security | Database Encryption | Database Assessment | Database Activity Monitoring | CASB - DLP | Data Loss Prevention | Storage DLP | Database DLP | Physical Media Control | Network DLP | Endpoint DLP | Content Discovery | Email DLP | Web Gateway DLP | Encryption | File/Folder | Email Encryption | SAN/NAS Encryption | Application Encryption | Access Management | Entitlement Management | File Activity Monitoring | Logging and Monitoring

Identity And Access Management

Directories | Directory replication | Directory Authentication and Authorisation | Recertification and Toxic Combinations | Role Based Access | Incompatible Role definition | Toxic combination detection | Access Recertification | Provisioning | Joiners, Leavers and Movers | Device Identities | Authoritative Source | Managing Generic Accounts | Federation | Browser Based Federation | Web Services | Authentication (Single and Multi Factor) | Web (forms, BA etc) | Enterprise | Certificates | Remote Access authentication | Biometrics | Mobile device | Network authentication (802.1x, PPAP, CHAP etc) | Challenge Response | Push Notification Authentication | Tokens (u2f, FIDO 2) | Privilege User Management | Logging and Monitoring | Authorisation | DMARC Email Authentication

Virtualisation

Access Control | Segregation Control | Resource Utilisation Management | Shared Storage | Virtualisation Infrastructure security | Virtual Networking Security | Logging and Monitoring

Security Management

Security Operations Tooling | SIEM | Log Investigation and Management Tooling | Security Operations Centre Tooling | Response and Investigation Case Tooling | MI, Dashboard and Compliance reporting | Cyber Intelligence (Situational Awareness) | Vulnerability Management | Penetration Testing Toolset | Vulnerability Scanning Toolset | Crypto Management | PKI | Secure Shell (SSH) | Key Management (Non PKI) | System Management | Patching | Configuration Management | Security Incident Management | Forensics | Computer Forensics | Malware Forensics | Business Continuity | Disaster Recovery Testing and Tooling | Business Continuity Management Tooling | Service Continuity Tooling

Cloud Security

Conditional Access | Cloud Access Governance | Cloud HSM | Information Protection | VPN Gateway | Key Vault | API Gateway | DDoS Protection | Directory Services | Application Gateway | Cloud Firewall Appliances | Adaptive Application Controls | Threat Detection | Disk Encryption | Just in Time Access | Network Threat Detection | Cloud Hardening | Build Configuration and Control | Logging and Monitoring | Secure Dev Ops Tooling | Cloud Security Access Broker | Authentication | Data Tokenisation | Encryption | DLP | Logging | Single Sign On | Access Control | Enforcement

Application Security Controls

Auditing | Application - Business Activity Logging | Application - Operational Support Activity Logging | Application Component Activity Logging | Access Control - Authorisation | ACLs - File system | ACLs - Database | Role Based Access Model | ACL's - Bespoke | ACL's - Client (Hosts allowed to use) | Application Logic controlled access control | Least Privilege controls | Incompatible Role Definition and Toxic Combination Detection | Separation of Duties | User and Application Authentication | Web (Forms, BA) | Browser based Federation (SAML, ADFS) | Application Federation (Web Services) | Bespoke Authentication | Directory (LDAP) | Unsuccessful Login Controls | Previous Logon Notification | Denial of Service Protection | Single Sign On | Encryption within the Application | Application Encryption | Channel Encryption (TLS, etc) | Credential Encryption | Session Management | Session Termination | Session Lock | Session Auditing | Concurrent Session Control | Session Authenticity | Integrity Controls | Tamper Resistance and Detection | Memory Protection | Input Validation (bounds checking etc) | Code Control | Data at Rest integrity controls | Partitioning | Application Code Partitioning | Application Partitioning | Security Function Separation

Security Testing and Code Validation

Application Testing | Dynamic Testing Tooling | Static Testing | Composition Analysis | Secure Development | Code Repository Tooling | Code Control Tooling | Automated Code Packaging and Deployment Tooling | Code Security Tooling | Web Application Assessment | Web Vulnerability Scanning | Web Application Testing Tools | Web Application Testing | Managed Services | Assessment/Testing | Managed Web Application Firewall

Operational Security Capability

Cloud Monitoring | Data Loss Prevention | Build Compliance | Vulnerability Scanning | Incident Management | Protective Monitoring | Privileged User Management | Patch Management | Remote Access Management | Anti Malware Management | Business Continuity Management | Key Management | Cloud Security Insight | Certificate Management | Internal Certificates Management | External Certificates Management | Intelligence | Security Advisories and Notifications | Brand Management | Regulatory Advisories | Security Testing | Internal Vulnerability Scanning | External Vulnerability Scanning | Annual Infrastructure Penetration Tests | Ad Hoc Infrastructure Penetration Tests | Annual Application Penetration Tests | Ad Hoc Application Penetration Tests | Red/Purple/Blue Team Testing | Security Operations Centre | Security Monitoring | Security Incident Management | Continuous Improvement | Threat Hunting | Misuse and Abuse Case Development | Security Test Management

Risk Management, Compliance and Governance

Governance and Compliance Management | C2M2 | SOX | PCI | ISO 27000 | GDPR/Data Protection Act | COBIT | NIST | C2M2 | ISF (SOGP) | Other | Security Policy, Standards, Guidelines, and Patterns Management | Education and Awareness | Security Risk Management | Validation and Maturity | Secure by Design | Supplier Risk Management | Design Assurance | Operational Risk Management

Service Management Capability (based on ITIL descriptions)

Software Version Management | Asset and Configuration Management | Backup and Recovery | Network Management | Licence Management | Change and Release Management | Problem Management | Service Level Management | Service Continuity Management | Deployment Compliance | Release and Deployment Management | Cloud Monitoring and Management | Testing | Release Management | Continuous Service Improvement