|  |  |  |
| --- | --- | --- |
| Computer  AH  SD.01 - All components, dependencies, and resources are **identified and confirmed** as needed.  SD.02 - The system must always **fail closed** or secure by default.  SD.03 - A **Threat model** of the system has been completed (e.g. STRIDE, or OWASP Cornucopia).  SD.04 - The system considers and mitigates the latest **OWASP Top 10**.  SD.05 - All Operating Systems must be **Hardened**.  SD.06 - All Operating System and Software must be kept **up to date and patched** accordingly.  SD.07 - All sessions are **securely managed**.  SD.08 - The system is **regularly scanned** using a Security Testing tool (e.g. IBM Rational App Scan).  SD.09 - **Anti-Virus Software** must be used to protect against malware.  *The Secure Development card focuses on general secure software development principles and good practices.*  Secure  Development |  | Diploma  AH  AN.01 - All passwords follow a **strong password** policy.  AN.02 - The system must enforce users to **change passwords** after a set number of days.  AN.03 - All use of PKI Certificates follows X.509 **Standards**.  AN.04 - **Initial or default** passwords must be changed.  AN.05 - The use of privileged accounts must be **restricted**.  AN.06 - The system must lock a user out after a set number of **failed login attempts**.  AN.07 - Forgotten password functions don’t reveal the current password, and use a **secure token** to allow account recovery.  AN.08 - All functions such as change password, or change email address, use the **initial** authentication mechanism.  AN.09 - **Multi-Factor** authentication approaches are used to enhance security.  AN.10 - The system must enforce Authentication controls on the **server side**.  AN.11 - A generic "**Invalid Credential**" message will be displayed to users who do not supply a valid credential.  Authentication  *The Authentication card involves ensuring the identification credentials provided are validated and verified.* |
| CheckmarkUnlock  AH  *The Authorisation card ensures that the Authenticated user can access the service or data they are requesting.*  AS.01 - The system uses **Whitelist** approaches in favour of Blacklists.  AS.02 - The system must use the principle of "**least privilege**".  AS.03 - The system validates that a user is authorised for the **service** they are requesting.  AS.04 - The system validates that a user is authorised for the **information** they are requesting.  AS.05 - There is a **centralised mechanism** for enforcing authorisation decisions (e.g. Windows Active Directory).  AS.06 - Verify that the access controls enforced are **consistent** on both the client and server side.  AS.07 - The system must enforce Authorisation controls on the **server side**.  Authorisation |  | Checklist  AH  *The Validation card focuses on ensuring information is transmitted or transferred securely.*  VL.01 - All input to the system must be validated against an **accepted whitelist** (e.g. users can only enter Alphanumeric characters up to a fixed length).  VL.02 - The system must enforce Security Focused Validation controls on the **server side**.  VL.03 - All application text must be **escaped** before return.  VL.04 - Batch input to the system must be validated against a **specified schema**.  VL.05 - Verify all database queries are **parameterised** to avoid injections.  VL.06 - The system must validate all **path and directory** traversals.  Validation |
| Key  AH  Encryption  *The Encryption card focuses on managing and implementing cryptographic controls.*  EN.01 - **Next Generation Encryption** algorithms must be used, avoiding any depreciated legacy algorithms.  EN.02 - When hashing passwords use a **salt value**.  EN.03 - When hashing passwords use **SHA-256 or SHA-512**.  EN.04 - Only **TLS1.2** web transfer technology can be used, disabling depreciated transfer technologies such as TLS1.1, TLS1.0, and SSL3.0.  EN.05 - All cryptographic keys are securely **managed, stored, and transferred**.  EN.06 - Verify that all random numbers, names, or strings are generated using the cryptographic module’s approved **random number generator**. |  | Magnifying glass  AH  Monitoring  *The Monitoring card focuses on detection, logging, and accountability to ensure non-repudiation of events.*  MN.01 - All human create, read, update, and delete (CRUD) **actions** must be logged.  MN.02 - Logs must be stored **externally** to the source system.  MN.03 - All successful and unsuccessful **authentication** attempts must be logged.  MN.04 - All successful and unsuccessful **authorisation** attempts must be logged.  MN.05 - There must be no security **sensitive information** displayed in logs.  MN.06 - Only the **appropriate information** must be contained in logs (e.g. User ID, Activity, and Timestamp).  MN.07 - Only **authorised people** can access specific logs. |
| CheckmarkSingle gear  AH  RL.01 - Component failure must not result in **service loss**.  RL.02 - Component failure must not result in **data loss**.  RL.03 - A **large incoming message** must be handled without system failure  RL.04 - **Large transaction volumes** must be handled without systems failure.  RL.05 - **Disk failure** must not result in data loss.  RL.06 - Message or Data **outside of expected** values must be appropriately handled.  *The Reliability card aims to ensure that the system consistently performs according to its specifications.*  Reliability |  | Wi-Fi  AH  *The Availability card focuses on ensuring the system services and information remain accessible.*  Availability  AV.01 - The system must meet its **Availability target** of \_\_\_\_\_%.  AV.02 - A regular **Backup and Recovery** strategy must be enforced.  AV.03 - A **Disaster Recovery** strategy must be enforced.  AV.04 - Disaster Recovery must **Failover** in \_\_\_\_\_ hours.  AV.05 - Disaster Recovery must only **lose** \_\_\_\_\_ minutes of information.  AV.06 - **Single point** of failures must be avoided in the system.  AV.07 - **Multiple instances** of each component must be deployed for resilience. |
| Gauge  AH  *The Performance card ensures your system can handle appropriate volumes with acceptable response times.*  PR.01 - An **incoming transaction** must be completed in \_\_\_\_\_ seconds.  PR.02 - A user’s **interactive request** must be responded to within \_\_\_\_\_ seconds.  PR.03 - The system must be able to handle **peak traffic** of \_\_\_\_\_ transactions per minute.  PR.04 - The system must be able to **store** \_\_\_\_\_ amount of data.  PR.05 - The system must handle **transaction messages** of a size up to \_\_\_\_\_.  PR.06 - The system must be able to **scale** to handle increased volumes of \_\_\_\_\_% within a period of \_\_\_\_\_.  Performance |  | Database  AH  DM.01 - A **Data Retention and Deletion** strategy must be in place for Application information.  DM.02 - A **secure destruction** strategy must be in place for Hardware.  DM.03 - The system must **avoid duplication** of data.  DM.04 - Sensitive data may be **encrypted at rest**.  DM.05 - Sensitive data may be **encrypted during transmission**.  DM.06 - **Protective Markings** must be appropriately applied to all stored data.  DM.07 - The system must be compliant with the **Freedom of Information** Act 2000.  DM.08 - The system must be compliant with the **General Data Protection Regulation** 2018.  *The Data Management card aims to ensure that the data held within the system is handled appropriately.*  Data  Management |
| Gears  AH  SM.01 - A component failure event must be **alerted** to the support team.  SM.02 - A system patch/upgrade must be able to be installed with **downtime** of no more than \_\_\_\_\_ mins.  SM.03 - The installed **configuration** must be capable of being easily determined for baseline management.  SM.04 - All transactions must be **logged** to allow for problem determination.  SM.05 - **License compliance** must be demonstrable.  SM.06 - The support team must be able to **report** on meeting response time targets.  SM.07 - The support team must be able to **restore the system** from a backup to a consistent state.  System  Management  *The System Management card aims to ensure that the system can be run and managed.* |  | Lightbulb  AH  OT.01 - Data must be **deleted** after \_\_\_\_\_ years to meet data retention requirements.  OT.02 - System must meet **regulation** \_\_\_\_\_ (specific to industry).  OT.03 - The system must be usable by people with **colour blindness**.  OT.04 - The system must be usable by people **with limited eyesight**.  OT.05 - The system must **not flash** more than 3 times in a 1 second period.  Other  *The Other card focuses on any other NFR areas.* |