| **#** | **Requirement** | **Details of Implementation** |
| --- | --- | --- |
| Setup | Ownership and Criticality of the System:  Business Owner (Name, Department and Designation);  IT System Manager (Name, Department and Designation);  Project Manager;  Project Name;  Cost Charge Code;  Confidentiality, Integrity and Availability rating of the System (Define Worst Case Impact if each of the components is affected).  Availability rating should determine the RTO and RPO of the system. |  |
| Setup | Describe the scope of change introduced by the project.  Describe the purpose of the system and its functions.  Describe the user base of the system. |  |
| Setup | Provide inter-system (between different systems) connectivity diagram.  Provide intra-system (within the system) connectivity diagram.  Indicate the Datacenter (DC) where each system is hosted. |  |
| Setup | Data-In-Motion Encryption – All data transfer from component to component should be using secure protocols which provides encryption of the data being transferred (SFTP, FTPS, Secure-JDBC, SSL, SSH, etc) |  |
| Setup | Data-At-Rest Encryption:  Option 1 – Application Server level encryption of data before storing into Database (Application administrators have full access to data)  Option 2 – Database level encryption of data (Application administrators and DBAs have full access to data).  Option 3 – Disk/SAN level encryption of data (Application administrators, DBAs and OS administrators have full access to data). |  |
| Setup | Password Controls:  Password should enforce the inclusion of Uppercase, Lowercase, Number and Symbol. Enforce the non-usage of past 10 passwords. Enforce password expiry for every 90 days. Passwords must use a minimum of 15 characters.  [Guidance: Use Passphrases instead of a word. Example: IHave1cat&ILoveIt! ] |  |
| Setup | Two-Factor Authentication should be used for access to application/systems over the Internet. The second factor being SMS OTP or Hardware Token OTP. |  |
| Setup | Transaction Signing (OTP generated from Hardware Token based on input value related to the transaction or input value sent through SMS) should be used for authorizing financial transactions and for changing of critical customer data, over the internet. |  |
| Setup | Session Inactivity:  (i) [Optional] The session should be locked after a pre-defined period of inactivity;  (ii) The session should be logged-out after a pre-defined period of inactivity; |  |
| Setup | Confidential data at Endpoint Devices:  Confidential data should not be stored into disk storage in Endpoint devices, without a strong Need-To-Have. If there is a strong Need-To-Have, the data should be stored into Encrypted Containers and the Integrity of the Container should be verified before the data is re-used by the application. |  |
| Setup | Cache at Endpoint Devices:  Cache used in endpoint devices should be cleared when the application logs out. |  |
| Setup | Critical Processes at Trusted System:  Input Validation, Output Encoding, Authentication, Authorization, Session Identifier Creation, Cryptographic Functions to protect secrets from Application User and Logging Controls should be implemented at the Trusted System - at the Server side; and not at the User Endpoint.  Authentication should be required for accessing each page and resource at the server side, unless public usage is intended. |  |
| Setup | Access Control:  Please provide Access Roles-Permissions Matrix (including Business and IT). Please indicate which Roles are classified as Privileged Roles. |  |
| Setup | Security Logging:  Process for recording, protection, retention, ~review of security logs (login/logout, change to access rights, security configurations, etc) should be established. |  |
| Setup | Activity Logging:  Process for recording, protection, retention and ~review of activity logs should be established. |  |
| Setup | Secure Coding Practices:  Use OWASP Secure Coding Practice Quick Reference Checklist during code development and review. |  |
| Setup | Integrity of Golden Source Data:  Any data that is received by the application to be used as a golden source should be integrity verified by the Business Owner. |  |
| Setup | Network and Application Penetration Testing:  Internal Network and Application Gray Box Penetration Testing should be performed for Internet Facing Systems and Critical Internal Systems before Go-Live. |  |
| Setup | Platform Vulnerability Assessment:  Platform (OS, DB, and Device) vulnerability assessment should be performed before System Go-Live. |  |
| Setup | Anti-Malware Protection:  Anti-Malware Solutions should be installed on all Wintel Platforms supporting the System. |  |
| Setup | Support Documentations:  Documentations should be created to ensure that there is adequate information to support ongoing operations, problem resolution and future maintenance of the system. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |