Reserve Bank Information Technology Pvt Ltd

Application Security Framework

Abstract

This document is a practitioner's guide for CISOs to implement application security within their organization. The aim of the document is to provide a logical flow and process to carry out application security best practices.

Author/Contributors

Author	Murli Nambiar
Contributors	Abhishek Tripathi
	Krunal Patel
	Manish Nagle
	Pankaj Patil
	Prajakta Sharma
	Sanjay Jain
	Seema Gamre
	Shailender Rajput
	Tabish Shaikh

Contents

Executive Summary

One of the key domain a Chief Information Security Officer (CISO) needs to tackle from security perspective is application security. The CISO should have a comprehensive strategy on application security which can survive the cyber onslaught that organizations experience on day to day basis. With all the protection solutions implemented within the organization and its perimeter, if the basics of application security are not addressed, the possibility of some malicious actor compromising the organization is very high.

There are several documents and articles relating to this domain, however they do not address the issue comprehensively. CISOs have grappled with not having a concerted approach towards addressing the risks in this critical domain. This document is a practitioner's guide for CISOs to implement application security within their organization. The aim of the document is to provide a logical flow and process to carry out application security best practices, some of the domains would need frameworks of their own, for ex: Risk assessment.

The security team would need to define the procedures for various activities defined in this document or may possibly already have it defined as per their ISO 27K certification procedural requirements. This document doesn't claim to be all encompassing and may not cover some aspects. We look forward to feedback from the community so it can be strengthened further.

1. How and where do we start?

Any application has three critical components which interact closely, primarily the application itself, the database where the data is stored and the front end web component. In this document we will concentrate on the first two elements.

For any organization, the key aspect to identify is whether they have skilled resources in this space. As the domain itself is vast, there is a need to have specialized resources covering each aspect. The skill sets needed are:

- Secure Software Development Life cycle (S-SDLC) expert
- Risk assessment team
- Vulnerability assessment and Penetration testing
- Application security sustenance team
- Access security
- Database security
- SOC team
- Forensics team
- Network security team

Some of the in-house team members may have these skills or it may be outsourced to third parties. In addition, some resources may be skilled in one or more areas. However, even in a moderately sized organization the count of new/existing applications is usually high enough to warrant dedicated resources to the task.

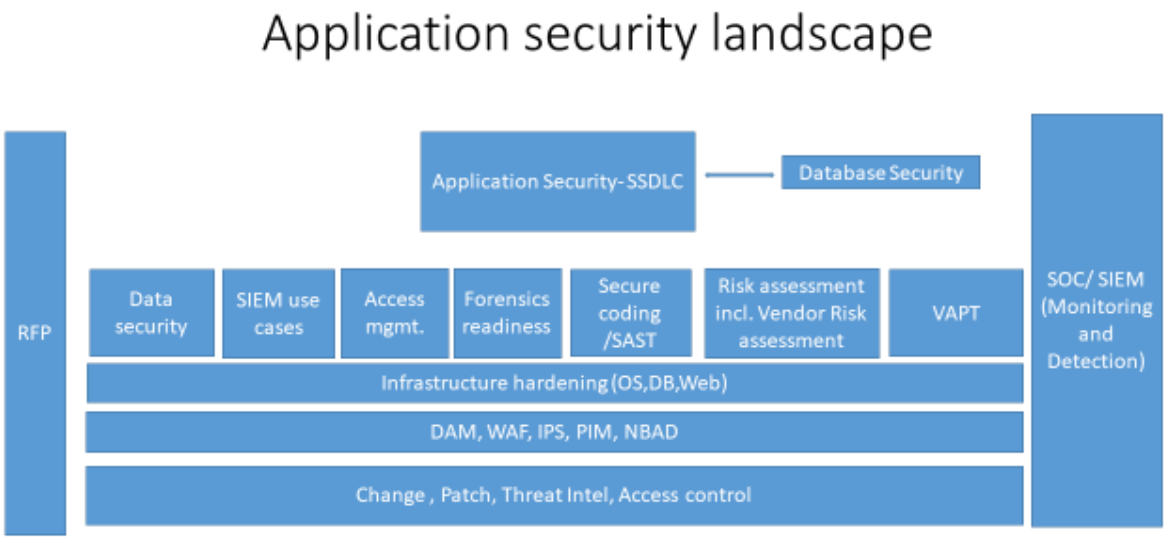
In addition to the above, the security team should be well-versed with the procurement process. We shall cover this in detail later. Once the resources are in place, the framework defined below could be a stepping stone to implement security.

2. Application security life cycle

Application development starts with the business teams expressing a need to automate some business process to either enhance productivity or implement a new idea for business. The IT team is approached to address the requirement. The IT development teams review the requirement & decide whether an application can be developed or procured.

The development could be done by internal IT teams or outsourced to third parties. The S-SDLC forms an integral component during the development life cycle of the solution. While IT teams would follow the SDLC framework, the security team would incorporate the 'Secure' aspects in the lifecycle. The application security team will call on other security teams during the process as and when needed.

The application security landscape in this case is given below to provide a high level view of the same:



2.1 Request for Proposal / Procurement

If the development is outsourced to third parties, it's imperative to identify a vendor who has a high level of security maturity in their organization. For this, the RFP or other process used to evaluate vendors should mandatorily define the security requirements of the organization. Annexure A can be used as a sample template. There are cases where vendor may not have adequately trained development resources on security, in which case it should be mandatory for them to use Static application security testing (SAST) tools and provide a report on the code security.

This aspect should be captured in the RFP. The 'Right to Audit' clause should also be incorporated into the RFP. This is an important clause so the vendor risk assessment process can be carried out. During the evaluation process, adherence of the vendor to the RFP clauses should be vetted. Adequate weightage should be accorded to this section in the evaluation process.

2.2 Development life cycle

The business teams prepare the Business Requirement Document (BRD) capturing the various aspects of the functionality needed in the new application. The IT development team, based on the BRD, prepares the System Requirement Specification (SRS) document which is vetted by the business teams and signed off. The development process would follow the Secure Software Development Life cycle process as detailed in Annexure B.

a. **Risk assessment** - During the SRS preparation, the cyber security team should carry out threat modelling and risk assessment of the proposed application. The solutions to address the risks should be defined and included in the SRS for the developers to consider in their design, code and build phases. The risk team should create the risk register capturing the risks and suggested solution. This risk register should be the key input to be considered when the final risk assessment is carried out prior to production rollout. The application risk assessment would cover the application functionality and associated threats. The process to be followed would be as per the risk assessment methodology or framework defined by the organization, possibly as part of their ISO 27K certification or using ISO 31000:2018.

In addition to the application risk assessment, a first level Vendor Security Risk Assessment (VSRA) should also be initiated. The assessment would require the VSRA team to visit the vendor's location where development would be carried out. The objective of this process is to review the practices adopted by the vendor to develop code for the organization, identify risks and suggest recommendations to plug the risks.

- Some of the key parameters to be reviewed during the VSRA process are:

    a. Vendor should follow Secure Software Development Lifecycle.
    b. Vendor should ensure only authorized users have access to the source code.
    c. The source code should be maintained in version controlled environment that provides for logging and audit of all activities performed on source code.
    d. All the tools used to develop/support the application should be access controlled.
    e. Development, test environment and production environment must be physically and logically separated from one another.
    f. All personnel who will be part of this engagement will need to signup NDA with the <organization>.
    g. A background verification needs to be done of all the personnel who will be part of this engagement.
    h. Test data shall be selected carefully, protected and controlled.
    i. The workspace used by the personnel's working on this project should be physically separated and access controlled.
    j. How would the final code be secured by the vendor, would it be with the organization or kept in escrow or stored with the vendor for future development requirements?
    k. The vendor risk report should be shared with business team/CISO for closure

Depending on the risk classification of the vendor, business may take a call to either wait till High/Critical points are closed or proceed with exception sign off.

b. **Access security** - During this process, the access security of the application should also be defined. Access control is one of the key components of any application and database. Most of the threats arise from poor access management process & procedures. Hence it is critical to have a detailed process in this regard.

   1) The access security team will define the access management module to be developed in the application. The access management module should cater to provisioning, change/transfer, de-provisioning and recertification process.

   2) The access process will define how users would connect & use the application. The users could be internal or external to the organization. The process will also define how change (when users' profile undergoes a change) and deletion of ID's (de-provisioning) would take place.

   3) The process would also define the're-certification' procedure for the application and supporting environment. Generic and Service accounts which are not monitored pose a big risk to the organization. Recertification process is the key to ensure no resigned user ID's remain or unauthorized user ID's have been created on the system or application.

   4) In addition, it will also cover access for the operating system administrator /users, database administrators/users and web administrators/users.

   5) In organizations that have an Identity and Access Management (IDAM) solution implemented, this process could be defined on the IDAM.

   6) Access to the application, database, web and OS admin accounts should be configured through a Privileged Identity management (PIM) solution (where available).

c. **Logs and monitoring** - During this process, the logging capabilities of the application should be defined. The SOC team should be part of the application SRS walk-through and based on the risks identified by the risk assessment team, define the rules for monitoring & detection on the Security Information Event Management (SIEM).

d. **Forensics readiness** – In the eventuality of the application being targeted or even compromised it is important for the organization to be able to carry out forensics of the attack as part of its incidence response framework. In most of the cases, there are inadequate data points or logs available for the forensics team to carry out an effective investigation. Therefore, it is recommended to

develop the application and keep it ready for forensics, should the situation arise. The following parameters could be logged:

i. Login/logout (local and remote)
ii. Password change/Authentication change
iii. Authorization based events (Example: Authorization denied/accepted for specific module of the application)
iv. All commands/activities carried out by a privileged user account need to be logged.

- Configuration/code change in the application.
- Module insertion/deletion/modification
- Addition of the privilege or a non-privileged user
- Privilege modifications of configured users.
- Module or application restart.

At a minimum, following fields need to be present in every log record:

- Time Stamp: when recorded event has happened
- Application: Producer of log entry
- Users: information of user which has triggered an activity
- Session ID
- Severity: Informational/Major/Minor/Critical
- Event description: why something has happened
- Log categorization Audit/Access/Event

e. **Data classification** – The security engineering team should use this opportunity to identify the critical data that would be generated in the application. The identification of critical data is important for three important projects – Using in the Database Activity Monitoring (DAM) rules, encrypting in Document Rights Management (DRM) /Information Rights Management (IRM) and fingerprinting on Data Leak Prevention (DLP) systems. While a detailed Data flow analysis (DFA) could be carried out subsequently, which is an important pre-requisite for any DRM/IRM implementation, identification and classification of critical data as per the organization's security policy during this process can provide an early lead.

f. **Code testing** – During the development of the application, periodic testing of the code using Static Application Security Testing (SAST) tool should be carried out. The SAST tool can be executed either by the vendor (if already incorporated into the RFP evaluation process) or by the organization's cyber security team. The vulnerabilities identified during this testing would be plugged by the development team. The vendor should be advised to share the report and its closure status with the organization's cyber security team.

g. **Change management process** – It is quite possible there could be business level changes that may arise during the development cycle. It is important to ensure none of these changes lead to new unforeseen risks. To mitigate this risk, all changes should be reviewed by the security risk assessment team for possible risks. If a new risk arises, the risk register should be updated with the suggested solution.

2.3 Production rollout

Once the application is ready for UAT, four teams play a major role at this stage:

1) **Risk Assessment (RA):** The RA team would review the application in entirety and confirm all the risks identified in SRS review process have been plugged. In addition, they would carry out an exhaustive risk analysis of the application including reviewing the change requests that were generated during the development process and reviewing the updated risk register to ensure no new risks have been discovered.

   - **Application and infrastructure risk assessment:**

     The RA team should cover the following areas at a minimum during the risk assessment phase:

     a. Design / Architecture risks
     b. Infrastructure risks – OS, Network (Firewall, Remote access, Router), End points
     c. Interface risk
     d. API risk
     e. Open source software risk
     f. User authentication / authorization risk
     g. User management risk

h. Data security risk (encryption, at rest, in transit, PII)
i. Data access risk
j. Monitoring risk (logging)
k. BCP risk (backup, DR site)
l. Change management risk
m. Technical support risk (skillful resource, software end of life)
n. Legal & regulatory risk

2) **Vendor security risk assessment (VSRA)**: The VSRA team would assess if the risks identified during the development phase have been closed in entirety or new risks have been identified. The objective of this step is to review the vendor preparedness in providing consistent services meeting the organization's information security requirements as defined during the RFP process. Some of the key areas to review are:

- Information security policies
- Human resources security
- Asset management security
- Security in access control
- Physical and environmental security
- Operations security
- Endpoint security – End User
- Endpoint security – Production/ Development server
- Security in development and support process
- Infrastructure security
- Security awareness
- Reactive security
- Proactive security - Independent third-party penetration testing
- Proactive security – Vulnerability management /Patching

3) **Vulnerability assessment and Pen testing (VAPT):** The VAPT team would carry out an exhaustive VAPT of the solution including a grey box, black box and white box testing. The VAPT team should carry out the following tests at a minimum:

- Grey box and White box testing
- Mobile application (if applicable)
- Web application VAPT
- Thick client app VAPT

- Underlying infra (Servers) VAPT
- Mobile app (Android) VAPT
- Mobile app (iPhone/ iPad) VAPT
- Windows app VAPT
- Handhold device application VAPT

The findings of the RA and VAPT would be shared with the development team to fix. The SAST tool would be run during this cycle to ensure there are no risks or vulnerabilities. There are scenarios when the identified risks and vulnerabilities may not be closed due to technical or financial limitations. It is imperative, the business leader signs off on the risks and submits the exception form/residual risk to the organization's CISO. These exceptions and residual risks should be highlighted to the SOC so they are aware of the same.

Once the application is tested and moved into production systems, it's recommended for the VAPT team to carry out a black box testing before launching the application. This confirms that the code tested in UAT is the actual code that's moved into production and no changes were introduced. The VAPT and RA team would provide the final risk and VAPT reports to the CISO with the sign off date. This baselines the application code, no changes should be carried out post this baseline testing before moving to production

4) **Security Operations Center (SOC):** The security operations team would then initiate the integration of the application with the various security solutions within the data center. Most of the data / information needed for the effective functioning of the solutions would have been captured during the initial SRS review phase and developed during the development phase.

I. **Web Application Firewall (WAF)** – During the UAT phase, the application should be integrated with the WAF. The WAF is a critical security solution deployed at the gateway level to detect web application attacks. The security team should analyze the traffic being used by the application during the UAT, this will help them to whitelist the traffic and block the noise / blacklist all other traffic.

II. **Intrusion Prevention System (IPS)**: The IPS solution provides the early warning indicator of any attacks on the application or infrastructure, which may have bypassed the WAF. During the UAT phase, the IPS logs will be reviewed & analyzed to identify false positives generated by the application. Following are the activities suggested:

- Understand application infra and platform on which it is running
- Collate IP details for application under review
- Carry out packet capture from IPS
- Analyze the packet capture to identify signature impact and its applicability to the application
- Analyze traffic to conclude on true positive or false positive events
- Submit report to datacenter/application owner for corrective actions.
- Maintain record of the same for future reference by internal teams.

III. **Database Activity Monitoring (DAM):** The DAM helps to monitor and detect attacks at the database level. Usually DAM solutions provide the following features – monitor, capture and record database events in near-real time and provide alerts about policy violations, define rules to identify any changes being done on critical data (as identified during the data security phase), run vulnerability scans on the database, real-time data masking helps to ensure that critical data does not fall into the wrong hands.

IV. **Privileged Identity Management (PIM)** – Access to the application admin ID, Database/OS/Web admin ID's, Generic and Service accounts should be provided only through the PIM solution. Ensure all direct access to the servers are disabled (not deleted) after the PIM is configured. The disabled direct access can be a backup should the PIM fail for any reason.

V. **Network Based Anomaly Detection (NBAD)** – This solution can be used to identify the normal traffic generated by the application. Rules could be written to trigger an alert on any abnormal traffic identified during the operations.

VI. **Integration with SIEM** – The application (Web) and infrastructure (OS) should be integrated with the SIEM. The SIEM rules should be written to cover potential incidents relating to the application and infrastructure events. During the initial review the SOC team would have gathered necessary details to identify the rules needed to identify incidents including residual or accepted risks communicated by CISO team. The OS should be configured to only capture relevant logs which are sent to the SIEM, based on the rules that are defined. This helps to reduce the noise and EPS count.

The DAM, WAF, IPS and PIM should be integrated with the SIEM solution, relevant rules to be defined for identifying potential incidents.

VII. **Hardening of Infrastructure** – The infrastructure used to host the application and database also needs to be secured to prevent vulnerabilities being exploited. Some of the key areas to cover are:

1. Operating system hardening (CIS benchmark is a good resource to review)
2. Database hardening
3. Web hardening

2.4 Post deployment processes

Once the UAT code is signed off and approved for use in production, the production support team will copy the code on production servers. Certain processes would need to be institutionalized to ensure the application security state is maintained.

1) **Change management** – A strict change management process should be carried out post deployment. This is critical to ensure subsequent changes don't create new security risks. This applies to both application and infrastructure level changes.

- The business / IT teams will submit the change request form, capturing the proposed change, impact to the system/application, criticality of the change etc.
- The cyber security risk team would assess the change and identify if a detailed RA or VAPT would be needed. In some organizations, there could be a formal Change Approval Board (CAB) in which the cyber security team should have a representation. The recommendations would be shared with the CISO.
- Based on CISO approval for the recommendations, the developers would initiate the development for the changes. The SAST tool would be used to assess the code security during the development process.

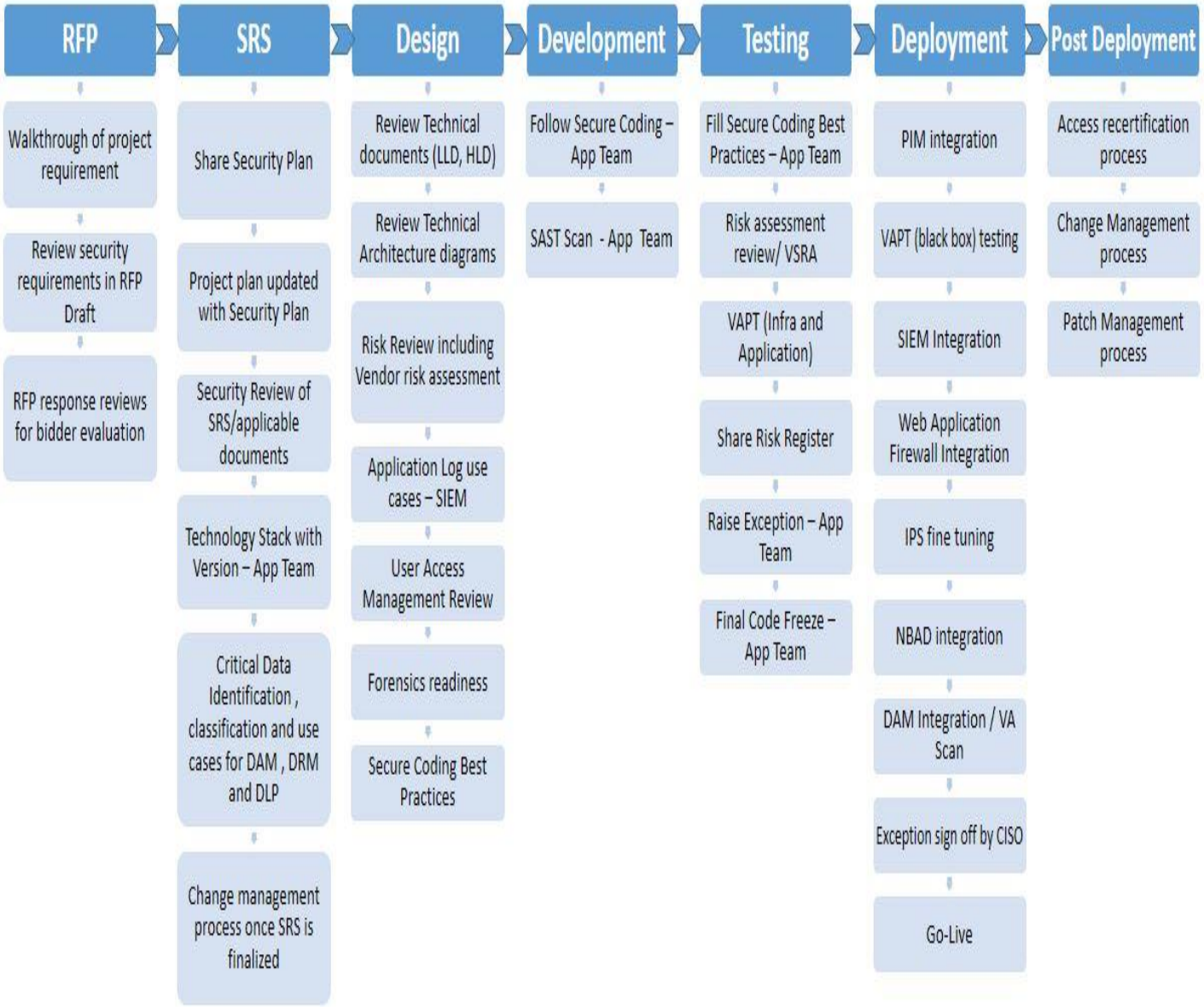
- On completion of the code development, the VAPT would be carried out. The VAPT report would be shared with the business team so that developers shall fix the same before going live. This is a cyclic process until the code is clear and can be moved to production.
- Some applications may undergo regular changes and it may be difficult to carry out VAPT for every change. The organization can take an informed decision based on the criticality of the change, possibly the medium and low changes could be tested once a quarter.
- It is important to identify any new data that is generated during the change process and ensure the business teams secure the same through DRM/IRM and/or DLP. The data flow analysis sheet should be updated with the same.

2) **Patch Management** – The technology landscape of the application should be captured during the risk assessment process.

1. The inventory of hardware, software, OS, DB, web, middleware and other tools used in development of the application would be shared with the Threat Intel / SOC team to subscribe to feeds relating to new vulnerabilities identified or new patches that have been released by the OEM.
2. The application and infrastructure team would then ensure patching of the environment as per the organization patch management framework and confirm the status to the SOC team.
3. The patching status should be recorded and managed by the SOC team. A monthly report on the same should be shared with the CISO of the organization for exception or residual risk sign off.

3) **Access recertification** – The recertification process of the access given on the application, DB, OS and web needs to be carried out on periodic basis. Based on the application criticality the recertification could be carried out quarterly, half yearly or yearly. The application and infrastructure owner should validate and confirm the access granted, record the same.

3. Various stages of the S-SDLC



4. Annexures

A. Security Requirements to be included in the RFP

1.1 Secure Design

a. Develop, implement, maintain and use best in class industry proven security controls that prevents the misuse of information systems and appropriately protect the confidentiality, integrity, and availability of information systems. Follow industry standards such as OWASP, SANS, NIST frameworks during design and development phase.
b. The platform should support strong authentication controls like multifactor authentication
c. The platform should have strong authorization controls. Solution to have controls for prevention against unauthorized data access and distribution. User and admin access control management to be provided as part of solution. Access control to be based on least access privilege principle. <Organization> or team assigned by <Organization> will be reviewing all access controls mechanism defined.
d. The solution should be capable of integrating with the existing single sign on facility of the <organization>.
e. While developing the interfaces, the Bidder must ensure and incorporate all necessary security and control features within the application, OS, database, network etc., as per OWASP, SANS standards so as to maintain confidentiality, integrity and availability of the data.
f. Wherever applicable, the solution to have strong file level validation controls for size, type and content. There should be preventive control against malware. Files should be scanned for any malicious content in a controlled sandbox environment.
g. The file store locations need to be secured. Strong cryptographic controls to be supported. Such controls should be compliant as per Industry standards such as FIPS-140, level 2. The encryption should support for data while in transit or rest. All encryption keys should be stored in secured location (such as HSM) with limited access as per NIST framework.

1.2 Secure Development

a. The solution should adhere to the S-SDLC (Secure System Development Lifecycle) process and practices as per <organization> IS policy.
b. Bidder to adhere to the security plan as per the S-SDLC activities and should incorporate it into the Project Plan before getting it approved from <organization>
c. Developers should be skilled in secure coding and OWASP Top ten vulnerabilities.
d. Code should be developed as per secure coding practices and reviewed to ensure the same.

1.3 Secure Deployment

a. The solution for sandbox type environment should be isolated from production environment where data originating from external source could be processed & validated for any malicious content/code before being sent to internal system.
b. All the hardware or required components should be shipped directly from OEM to <organization> premises.
c. Bidder should enforce process and policies such that only authorized users should have access to the source code.
d. Test data shall be selected carefully and protected and controlled.
e. The source code should be maintained in version controlled environment that provides for logging and audit of all activities performed on source code.
f. Development, test, staging and production environment must be physically and logically separated from one another as far as possible.
g. The solution should ensure there should be no data leakages by implementation of distributed programming frameworks. The solution should secure data storage and logs. Auditing should be enabled to track each activity.
h. All the underlying infrastructure components such as OS, servers (web, application, and database) or any product should be hardened on each environment before being made functional.
i. Logging should be defined properly so that in the eventuality of the application being targeted or even compromised it is important for the organization to be able to carry out forensics of the attack as part of its incidence response framework.
j. Bidder should provide the support for integration of the application with Web Application Firewall (WAF) and provide the requisite details to WAF Team for implementation of the same.

k. Bidder should provide the support for integration of the application with Intrusion Prevention System (IPS) and the requisite details to IPS Team for implementation of the same.

l. The bidder should provide support for integration with SIEM (Security Information and Event Management), DAM (Database Activity Monitoring), and other available tools.

1.4 Security Assessment

a. Wherever applicable, the bidder to conduct SAST (Static Application Security Testing) & DAST (Dynamic Application Security Testing) and provide detailed reports of the same or <organization> may conduct the SAST. The bidder should close all the vulnerabilities which should be revalidated by conducting SAST & DAST again.

b. The bidder should provide full support to Security Review, VAPT and Risk Assessment of all platforms conducted by <organization>.

c. Standards Benchmark - To ensure that all parties have a common understanding of any security issues uncovered, the independent organization that specializes in Information security shall provide a rating based on industry standards as defined by First's Common Vulnerability Scoring System (CVSS) and Mitre's Common Weakness Enumeration (CWE).

1.5 BCP – DR

The selected bidder should develop a disaster recovery plan for restoration of the system in the event of a disaster or major incident. The Disaster Recovery (DR) Plan should be tested prior to the go-live to verify DR readiness. Ensure the promotion of the build to production environment is done in a secure manner and the production environment is ready for the system go-live.

1.6 Secure use of Open Source

a. The Implementation of open source technologies should be taken up in compliance with Information Security (IS) policy of the <organization>.

b. The bidder to provide full support in implementation and maintenance for the open source technologies in terms of upgradation, patching etc.

c. The bidder should provide the list of all open source libraries being used in the platform. None of these should consist of any malicious code/script. All such libraries/code should undergo SAST.
d. Developer shall disclose all binary executables (i.e. compiled or byte code; source code is not required) of the software, including all libraries or components.
e. Developer shall disclose the origin of all software and hardware components used in the product including any open source or 3rd party licensed components.

1.7 Security Compliance to Policies and Process

a. The Bidder shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems. Bidder will not copy any data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by <organization>.
b. The <organization> will have the right to audit the bidder's people, processes, technology etc. as part of Vendor security risk assessment process.
c. Solution should also be compliant to Indian Information Technology Act, 2000 (along with amendments as per Information Technology (Amendment) Act, 2008) and any applicable data privacy & protection Act.
d. The system should be fully compliant with ISO27001 controls.
e. All personnel who will be part of this engagement should agree to the terms and condition of NDA and sign in with the <organization>.

1.8 Security for Support & Maintenance

a. Bidder should follow all the process defined by <organization> like Incident, Change, Release and Patch Management
b. Static application security testing and dynamic application security testing should be conducted by the bidder for any change request involving a design or code change. All gaps identified will be fixed by Bidder prior to go-live.
c. <organization> reserves the right to conduct further security testing of the source code and the system by either <organization> personnel or another party. Any gaps identified during this testing will be fixed by Bidder at no extra cost to <organization>.

d. Configuration items such as computers and other devices, software & hardware contracts and licenses, third party tools and business services which are related to the application should be disclosed.
e. Bidder will resolve security incidents as per the agreed SLAs.
f. All user and technical access will be granted as per the Role Based Access Control (RBAC) matrix approved by <organization>. All access will be reviewed as per defined frequency and during control points e.g. when a team-member leave team or organization.
g. Information Security controls will be enforced when moving production data into non-production environments e.g. masking sensitive data during the cloning process etc. Audits will be conducted by <organization> to ensure security controls sustenance. Any gaps identified will be remediated by the bidder.

B. S-SDLC Procedures

During each of the SSDLC stage, different activities will be carried out. The description, required input documents and the final deliverables against each activity has been provided below.

i. Requirement Specification

Activity	Description	Inputs	Deliverables
Security planning	Initiate project security planning	1. Business Requirement Document 2. High level project plan 3. Data Classification	1. Security plan document 2. Project plan updated with security plan
SRS Security Review	Review SRS to identify security gaps	1. SRS 2. Other related documents	Security Review Report
Security Control	Define Security Specifications	Security Review Report	SRS updated with specifications as per security review report

Responsibilities –

Deliverable	Responsibility
Business Requirement Document	Application owner
High Level project plan	Application owner
Data Classification	Application owner
Security plan document	Information Security
SRS	Application owner
Security Review Report	Information Security
Updated SRS with comments as per security review report	Application owner

ii. Design

Activity	Description	Inputs	Deliverables
Security Architecture	Design Security Architecture	1. SRS 2. System Security Plan 3. Technical Architecture	Updated Technical Architecture document
Security Design	Review the build and deployment design document for security considerations. Identify variations from security plan	1. SRS 2. Technical Architecture 3. Build & deployment design 4. HLD/LLD 5. Technology Stack	1. Security Design Review document 2. Secure build and Deployment design

Responsibilities –

Deliverable	Responsibility
Technical Architecture	Application owner
Build & deployment design	Application owner
HLD/LLD	Application owner
Technology Stack	Application owner
Security Design review report	Information Security
Revised build & deployment design with security feedback	Application owner

iii. Development

Activity	Description	Inputs	Deliverables
Secure Coding	Aware Industry standard secure coding practice	1. Vendor coding standard/Practice 2. Industry standard secure coding practice references	Assurance of following secure coding practice (Application Teams)
Third Party Code	Identify if any third party code is to be used and create a list of best practices	List of all third party code/libraries to be used/API	Reviewed third party code/libraries/API and provide risk report
Secure Code review	Review the code from security aspect and find vulnerabilities	Application source code including any third party code/libraries	Secure code review report (SAST) from application development teams

Responsibilities –

Deliverable	Responsibility
Assurance of secure coding practice	Application owner
List of third party source code/libraries/API's	Application owner
Risk Assessment summary of Third Party code/libraries/API and best practices	Information Security
SAST Report	Application owner

iv. Testing

Activity	Description	Inputs	Deliverables
Assess System Security	Perform security risk assessment of the system and the environment it will be hosted in	1. Updated built and deployment design. 2. Risk assessment report 3. SRS 4. Technical Architecture 5. Application Walkthrough	Risk Assessment Report
Mitigate Risks	Perform risk mitigation measures as identified	Risk Assessment Report	1. Updates to Risk assessment report with status of mitigation measures 2. Exceptions document

Responsibilities –

Deliverable	Responsibility
Application walkthrough	Application owner
Risk Assessment Report	Information Security
Exception Document	Information Security

v. Deployment

Activity	Description	Inputs	Deliverables
VAPT	Perform VA-PT of the system in the proposed production environment or production-like environment	Security test scenarios	VAPT Assessment Report
Fix vulnerabilities	Close any vulnerabilities identified	VAPT Assessment Report	1. VAPT Assessment report after retest 2. Exceptions document
Security authorization	Authorize the production go-live of the Information System	1. Exception document 2. Risk Assessment Report 3. VAPT Report 4. DR Test results	Residual Risk Sign Off – Exception Document
Secure Deployment	Ensure the promotion of the build to production environment is done in a secure manner and the production environment is ready for the system go-live	1. Secure deployment checklist 2. Ecosystem security plan	1. Completed secure deployment checklist 2. Develop security monitoring SOPs

Responsibilities –

Deliverable	Responsibility
VAPT assessment Report	Information Security
Revised Exception Document	Information Security
Residual Risk Sign off	Application Owner
Secure deployment checklist	Information Security
Communicate residual risks/exceptions to SOC	Information Security
Security monitoring SOPs	Information Security
DR Drill results	Application Owner

vi. Support

Activity	Description	Inputs	Deliverables
Security Assessments	Perform periodic / need based security assessment, including risk assessment, vulnerability assessment and penetration testing of the system	1. System documentations 2. Servers inventory 3. Network architecture	Security Assessment report 1. Risk Assessment report 2. VA-PT Assessment report
Change Management	Perform security evaluation for changes to the system	Change Request document	1. CCB (Change Control Board) Decisions 2. Updated security documentations impacted by the change request

Responsibilities –

Deliverable	Responsibility
Periodic Risk Assessment Reports	Information Security
Periodic VAPT assessment reports	Information Security
Change Request Document	Application Team

STAY CONNECTED

Reserve Bank Information Technology Pvt. Ltd

https://rebit.org.in

LinkedIn
https://www.linkedin.com/company/reserve-bank-information-technology-pvt-ltd

Twitter
https://twitter.com/reservebankit

Email
communications@rebit.org.in

About ReBIT

Reserve Bank Information Technology Private Limited (ReBIT), has been set up by the Reserve Bank of India to serve its IT and cybersecurity needs and to improve the cyber resilience of the Indian banking industry.

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. ReBIT disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any act or omissions made based on such information. ReBIT does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel and other licensed professionals. The views, thoughts, and opinions expressed in this document belong solely to the author, and not necessarily to ReBIT.

Subscribe to ReBIT's Cyber Pulse Monthly Newsletter
https://rebit.org.in/newsletter