Secure SDLC approach

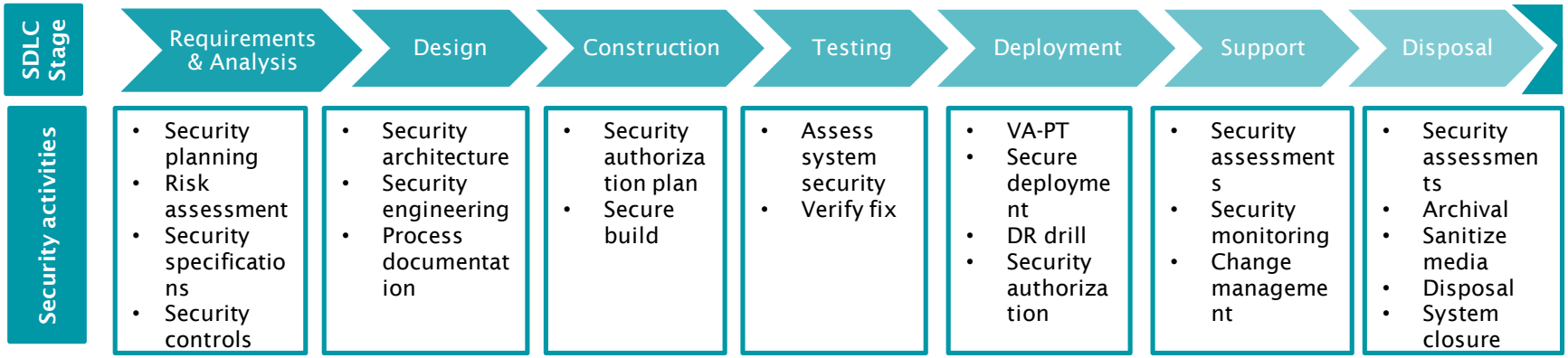
Version 1.1, 01-Nov-2017

रिज़र्व बैंक
सूचना प्रौद्योगिकी प्राइवेट लिमिटेड
Reserve Bank
Information Technology Pvt. Ltd.

Why Secure SDLC

- Evolving cyber threats make a focused security risk assessment imperative
- Cost of fixing a security defect increases exponentially at later stages of SDLC
- “Secure by design” provides for the best defence from cyber threats

Secure SDLC overview



Secure SDLC – Requirements & Analysis phase

Activity	Security planning	Risk assessment	Security specifications	Security controls
Description	Initiate project security planning	Assess risk to system	Define security specifications	Select and document Security Controls
Inputs	Business Requirements Document High level project plan IS data classification policy	SRS	Risk assessment report	SRS Risk assessment report
Deliverables	Security plan document Project plan updated with security plan	Risk assessment report	SRS updated with security specifications Secure technical controls	Ecosystem security plan

Stage gate	• Determine security acquisition strategy • System Concept Review	• Ecosystem security plan alignment • Risk Management Review

RACI – Requirements & Analysis phase deliverables

Document name	Stakeholders				
	CS	PM	Vendor	DIT	Business Owner
Project plan	C	R/A	R	C	C
Security plan document	R/A	I	I	C	I
Risk assessment report	R/A	I	I	C	I
SRS	I	A	R	I	C
SRS updates for security specifications	R/A	C	I	I	I
Ecosystem security plan	R/A	I	I	C	I

Secure SDLC – Design phase

Activity	Security architecture	Security engineering	Process documentation	Change management
Description	Design Security Architecture	Review the build and deployment design document for security considerations. Identify variations from security plan.	Process Documentations	• Perform Configuration Management • Perform Change management if any changes to the requirements
Inputs	• SRS • System Security Plan • HLD / LLD	• SRS • Ecosystem security plan • Security Architecture • Build & deployment design		• Change request documents
Deliverables	• Security architecture (part of System architecture document)	• Potential security test scenarios • Updated build & deployment design	• Additional security documentations	• Updated security documentations impacted by the change request

Stage gate	• Security Architecture / Design Review • Performance specifications review • EA Alignment	• Security test case review • Risk Management Review

RACI – Design phase deliverables

Document name	Stakeholders				
	CS	PM	Vendor	DIT	Business Owner
Security architecture	R/A	C	I	C	I
Potential security test scenarios	R/A	C	I		
Build & deployment design	C	A	R	C	I
Configuration management plan	C	A	R	C	I
BCP-DR Plan	A	C	R	C	C
Security monitoring plan	R/A	I	I	C	C
Incident response plan	R/A	I	I	C	I

Secure SDLC – Construction phase

Activity	Security authorization plan	Secure build	User awareness	Change management
Description	Create a detailed plan for security authorization	Integrate security into systems: · Coding reviews · Implement security controls	Create a user awareness strategy and training material	• Perform Configuration Management • Perform Change management if any changes to the requirements
Inputs	• SRS • Project scope • Business impact document	• Source code • System documentation	• User manual	• Change request documents
Deliverables	• Security authorization plan	• Code review reports / SAST reports	• Updated user manual for security awareness	• Updated security documentations impacted by the change request

Stage gate	• Security authorization review	• Code Review Reports/ SAST reports

RACI – Construction phase deliverables

Document name	Stakeholders				
	CS	PM	Vendor	DIT	Business Owner
Security authorization plan	R/A	C	I	C	I
Code Review Reports / SAST reports	C	A	R		
Updates to user manual with security awareness	R/A	C	I		C

Secure SDLC – Testing phase

Activity	Assess system security	Mitigate risks	Change management
Description	Perform a security risk assessment of the system and the environment it will be hosted in	Perform risk mitigation measures as identified	• Perform Configuration Management • Perform Change management if any changes to the requirements
Inputs	• Potential security test scenarios • Risk assessment report • SRS • Ecosystem security plan	• Risk assessment report	• Change request documents
Deliverables	• Risk assessment report	• Updates to Risk assessment report with status of mitigation measures • Exceptions document	• Updated security documentations impacted by the change request
Stage gate	• Security Assessment report review	• Exceptions document review	

RACI – Test phase deliverables

Document name	Stakeholders				
	CS	PM	Vendor	DIT	Business Owner
Risk assessment Report	R/A	I	I	C	I
Updates to Risk assessment report with status of mitigation measures	C	R/A	R/A	C	C
Exceptions document	C	R/A	R/A	C	C

Secure SDLC – Deployment phase

Activity	VA-PT	Fix vulnerabilities	DR drill	Security authorization	Secure deployment
Description	Perform VA-PT of the system in the proposed production env or production-like env	Close any vulnerabilities identified	Conduct Disaster Recovery drill prior to application go-live to verify DR readiness	Authorize the production go-live of the Information System	Ensure the promotion of the build to production environment is done in a secure manner and the production env is ready for the system go-live
Inputs	• Security test scenarios	• Security Assessment Report	• BCP/DR Plan	• Exceptions Document • Risk Assessment Report • VAPT Report • Completed secure deployment checklist • DR Test results	• Secure deployment checklist • Ecosystem security plan
Deliverables	• VAPT Assessment Report	• VAPT Assessment report after retest • Updated Exceptions document	• DR Test results	• Security Authorization • Residual Risk Sign Off	• Completed secure deployment checklist • Develop security monitoring SOPs

Stage gate	• Deployment Readiness Review	• Authorization Decision	• Final Project Status

RACI – Deployment phase deliverables

Document name	Stakeholders				
	CS	PM	Vendor	DIT	Business Owner
VAPT Assessment Report	R/A	I	I	C	I
Updated Exceptions document	C	R/A	R	C	C
DR Test Result	A	R	R	C	I
Security Authorization	R/A	C	I	I	I
Residual Risk Sign Off	R/A	C	I	I	C
Completed Secure deployment checklist	A	R	R	C	I
Develop security monitoring SOPs	A/R	C	C	C	C

Secure SDLC – Support phase

Activity	Security assessments	Security monitoring	Change management
Description	Perform periodic / need based security assessment, including risk assessment, vulnerability assessment and penetration testing of the system	Perform continuous security monitoring to detect threats, indications of compromise and intrusions Track the status of residual risks	Perform security evaluation for changes to the system
Inputs	• System documentations • Servers inventory • Network architecture	• Exceptions document • Monitoring SOPs	• Change Request document

Deliverables	• Security Assessment report
	  • Risk Assessment report
	  • VA-PT Assessment report
		• Updates to Exceptions document
		• Standard Operating Procedures:
		  • Change Management SOP
		  • Security Patch Management SOP
		  • Security Incident Response SOP
		  • Backup & restoration SOP
			• CCB Decisions
			• Updated security documentations impacted by the change request

RACI – Support phase deliverables

Document name	Stakeholders				
	CS	PM	Vendor	DIT	Business Owner
Security Assessment Report	R/A	I	I	C	I
Updates to Exceptions document	A	R	R	C	C
Change Management SOP	C	A	R	C	I
Security Patch Management SOP	A	R	R	R	I
Security Incident Response SOP	R/A	C	C	C	I
Backup & restoration SOP	A	R	R	R	I

Secure SDLC – Disposal phase

Activity	Security assessment	Archival	Sanitize media	Disposal	System closure
Description	Security assessment of Disposal or Transition Plan	Ensure information preservation	Sanitize media	Dispose of Hardware and Software	Close system
Inputs	• Disposal or Transition Plan • System documentation	• IS policy • Disposal or Transition Plan	• IS policy • Disposal or Transition Plan	• Disposal or Transition Plan • Decommission checklist	• Disposal or Transition Plan • Disposition Record
Deliverables	• Updated Disposal or Transition Plan	• Disposition record	• Updated disposition record	• Updated disposition record	• Completed decommission checklist

Stage gate	• Review of completed decommission checklist	• Review of Disposition record

RACI – Disposal phase deliverables

Document name	Stakeholders				
	CS	PM	Vendor	DIT	Business Owner
Disposition record	C	A	R	C	I
Update disposition records	C	A	R	C	I
Completed decommission checklist	C	A	R	C	I

Thank You