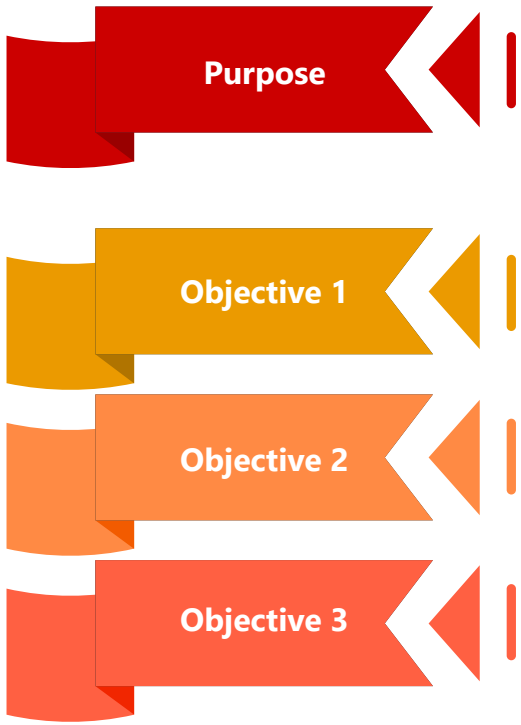
DBS Live more, Bank less

Security-by-Design Framework

Security-by-Design Framework

Purpose and Objectives of the SBC Framework

As a Critical Information Infrastructure Owner (CIIO), DBS is required to adopt the Security-by-Design (SBD) Framework as mandated by the Cyber Security Agency of Singapore (CSA).



Building security into their SDLC, through the alignment of security-related processes/activities alongside SDLC processes. This would result in more **cost-effective and risk-appropriate security considerations and controls** in all phases of the SDLC.

Establish SBD processes to ensure that **security risks are managed from the start, and continuously assessed** during the SDLC through a lifecycle approach.

Establish **activities** to support the SBD processes to **manage security risks during the SDLC**.

Provide control gates and decision point considerations at phases to ensure that **no decision is made without an assessment of the security risks**.

DBS

Overview of Security-by-Design

Framework provides approaches and guidelines to processes and activities within SDLC

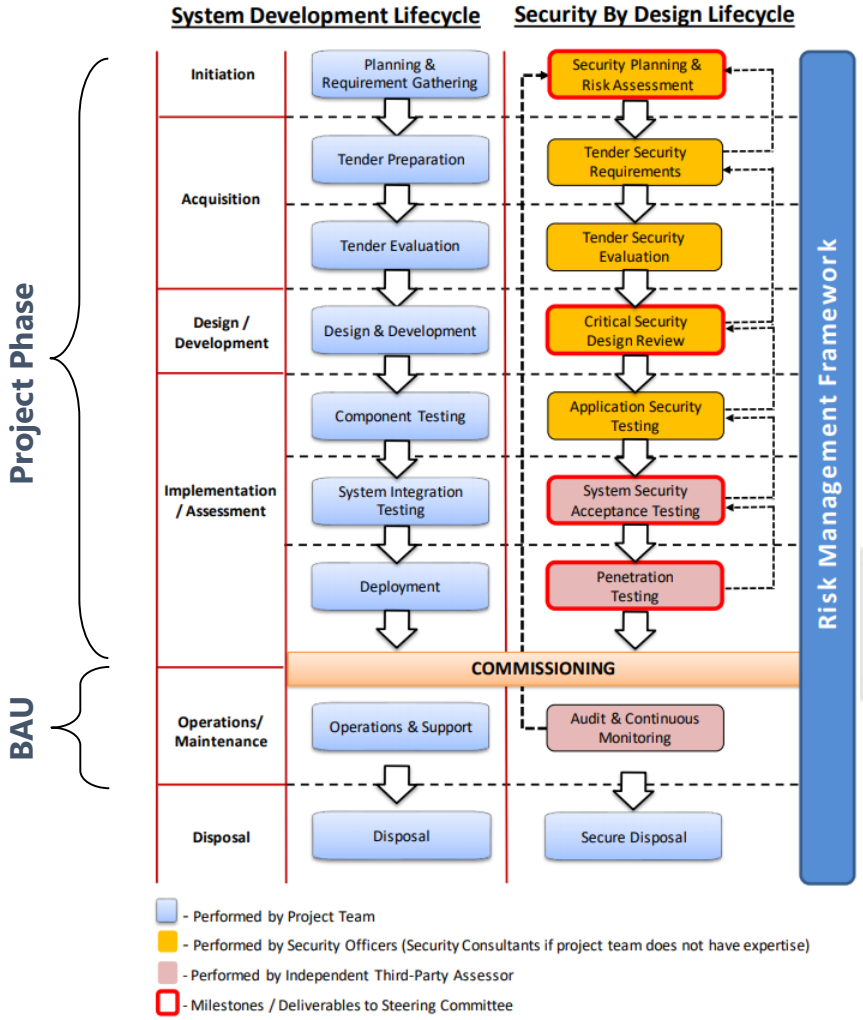
Security-by-Design Approach

The SBD approach consists of three components, namely,

a) **Lifecycle** – Aligning security-related processes with SDLC to guide projects to meet Security-by-Design objectives

b) **Activities** – Security-related activities that support the security lifecycle processes

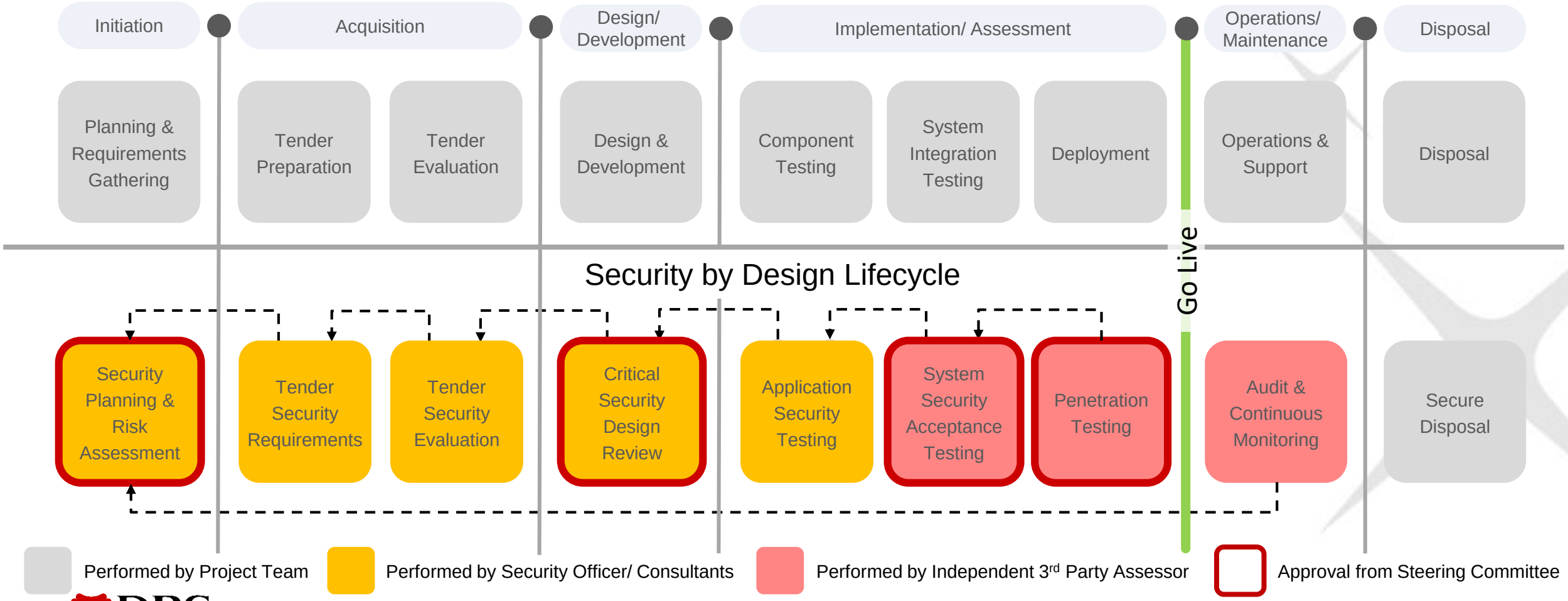
c) **Control Gates** – A point in time when the system development effort will be evaluated for security and when management will determine whether the project should continue as is, change direction or be discontinued



Security-by-Design Framework

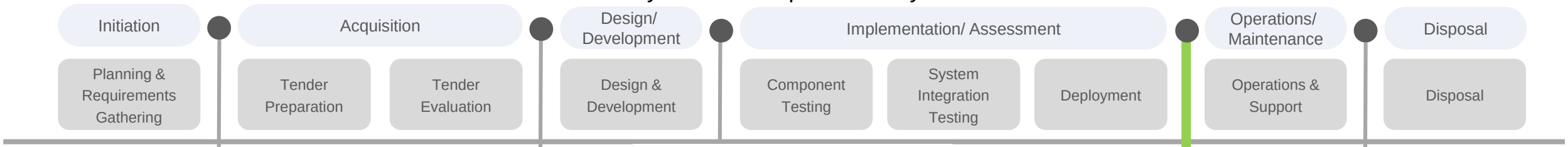
CSA mapping of SBC to SDLC

CIIO to adopt Security By Design Framework established by CSA to the extent that it applies to the CII's system development lifecycle (SDLC). The security design framework identifies key security activities for each phase of the SDLC and ensures that security needs are identified and implemented.

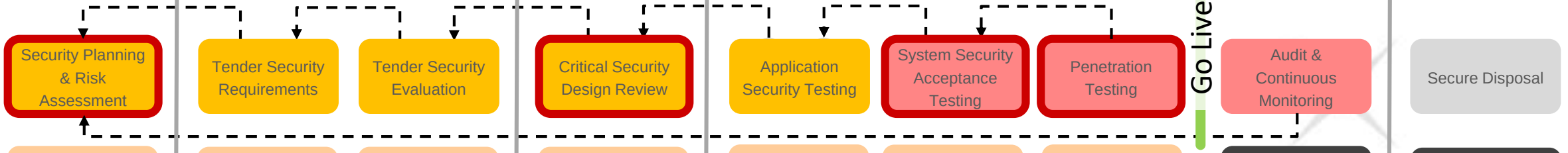


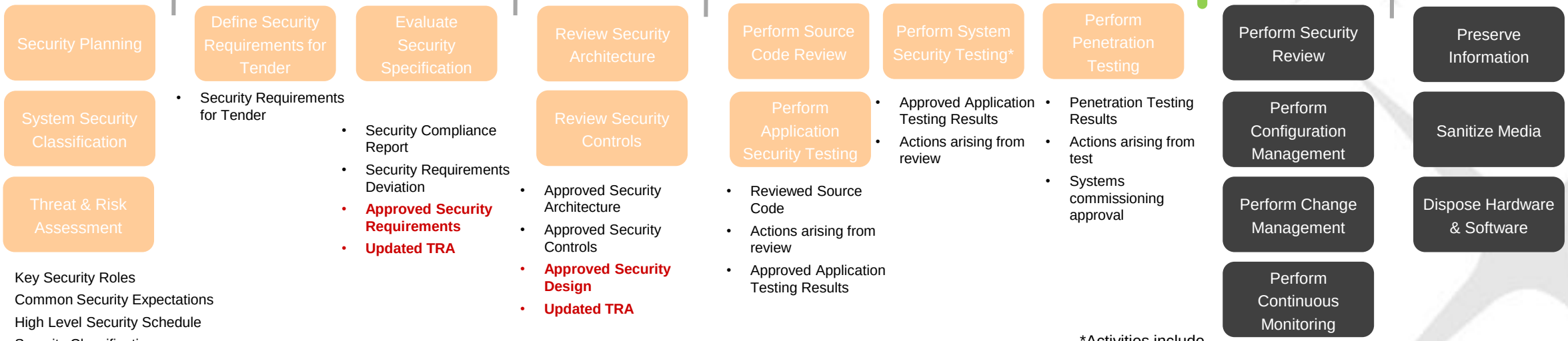
DBS

System Development Lifecycle



Security by Design Lifecycle





- Key Security Roles
- Common Security Expectations
- High Level Security Schedule
- Security Classification
- High Level Security Requirements
- TRA Report
- Updated Risk Register
- **Approved TRA Report**
- **Approved Security Roles & Responsibility**

- Security Requirements for Tender

- Security Compliance Report
- Security Requirements Deviation
- **Approved Security Requirements**
- **Updated TRA**

- Approved Security Architecture
- Approved Security Controls
- **Approved Security Design**
- **Updated TRA**

- Reviewed Source Code
- Actions arising from review
- Approved Application Testing Results

- Approved Application Testing Results
- Actions arising from review

- Penetration Testing Results
- Actions arising from test
- Systems commissioning approval

*Activities include

- checking of system configuration against security specifications and baseline standards (if any)
- Test case review (focusing on testing the security controls)
- Validation of acceptance test
- Assessment and recommendations

DBS

Performed by Project Team

Performed by Security Officer/ Consultants

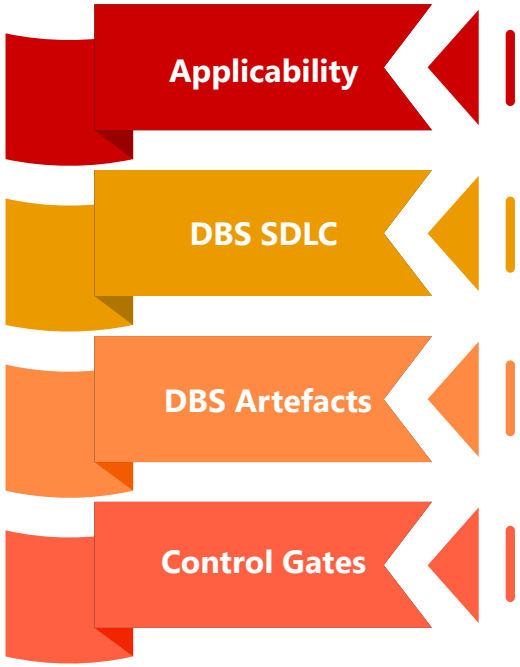
Performed by Independent 3rd Party Assessor

Approval from Steering Committee

Adhering to the SBD Framework

Key tasks performed to adhere to the requirements

In response to the SBD framework, alignment and changes has been made to the current process to adhere to the SBD requirements. A summary of the key tasks performed:



Established the applicability of SBD for all greenfield / initiatives that are more than SGD 500k. This is applicable to both application and infrastructure project.

SBD framework has been mapped to the DBS SDLC to align the framework to our internal process.

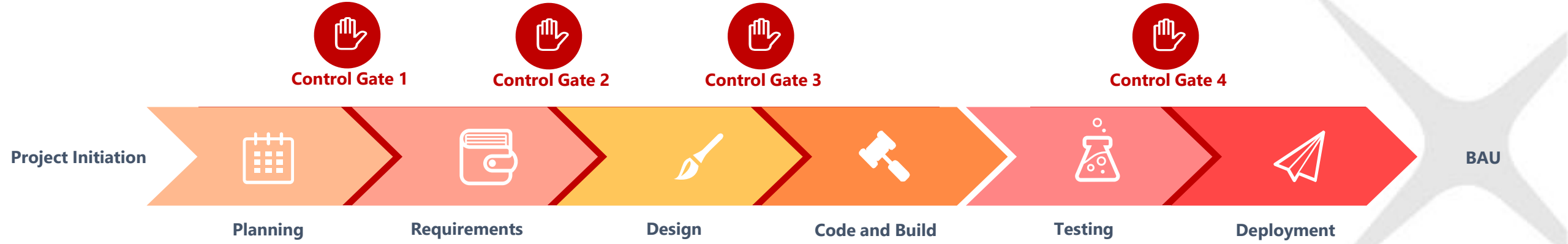
Artefacts to address the SBD requirements have been identified for the various phases of the SDLC process

Platform Governance Board (PGB) appointed as the control gate in response to CSA's requirement to establish control gates for various phases of the SBD framework

Project Phase

Phases and control gates in the **Project** phase

1) DBS has mapped our existing SDLC process to the SBD Framework and identified the required activities, artefacts and controls gates
2) Proposed control gates to manned by the **Platform Governance Board (PGB)**. Delegation of authority is allowed and must be clearly documented
3) Process if applicable for both Waterfall and Agile development methodology



Phase 1: Planning

Key Activities for the **Planning** phase

Security Planning

1) Project kick-off deck
2) Meeting minutes or approval

Security Classification

1) App Code Repository

Threat & Risk Assessment

1) TRA Report (contains Risk Register)

Control Gate

1) Project kick-off deck
2) Meeting minutes or approval
3) Security Classification and Availability Classification
4) TRA Report

DBS

Security Planning

Purpose

Establish the importance of incorporating security into the development lifecycle

Artefacts

1) Project kick-off deck
The deck should cover the following

- Establish common understanding of security goals and objectives
- High-level security schedule
- Security roles and responsibilities

2) Meeting minutes or approval

- From Application Manager / Project Sponsor

Reviewer

Application Manager / Project Sponsor

To be presented and approved during the project kick-off meeting

References

Being updated by Project Management (1 June)

DBS

Security Classification

Purpose

Define the security classification of the system and determine the security requirements

Artefacts

1) **App Code Repository**
   Security classification and availability classification to be updated in the App Code Repository

Reviewer

CISO Office

References

1) **Security Classification**
   Refer to the Information Classification and Handling Standard

2) **Availability Classification**
   Refer to High Availability and Disaster Recovery Standard

3) **App Code Repository**
   Update the classification to the App Code Repository

DBS

Threat and Risk Assessment

Purpose

Assess the application to identify threat and risk facing the application. Thereafter , determine that the risks identified have been adequately addressed (to an acceptable tolerance level) by the proposed security controls

Artefacts

1) **TRA Report (contains Risk Register)**
   Filled by project teams with guidance from ISS – Project Advisory

Reviewer

ISS – Project Advisory
Project advisory will provide guidance and review the TRA prepared by the project teams

References

1) **Template**
   Obtain the template for the TRA report through this link

2) **Request**
   Submit a request to schedule a review through this link

DBS

Control Gate 1

Control Gate for **Planning** Phase

Purpose

The purpose of this control gate is to ensure that security expectations are clearly spelt out and understood by the project stakeholders

Artefacts

1) **Project kick-off deck**
2) **Meeting minutes or approval**
3) **Security Classification and Availability Classification**

Gate

Platform Governance Board (PGB)
The PGB may assign a delegate to perform this role. The delegation must be clearly documented

DBS

Summary of Key Artefacts

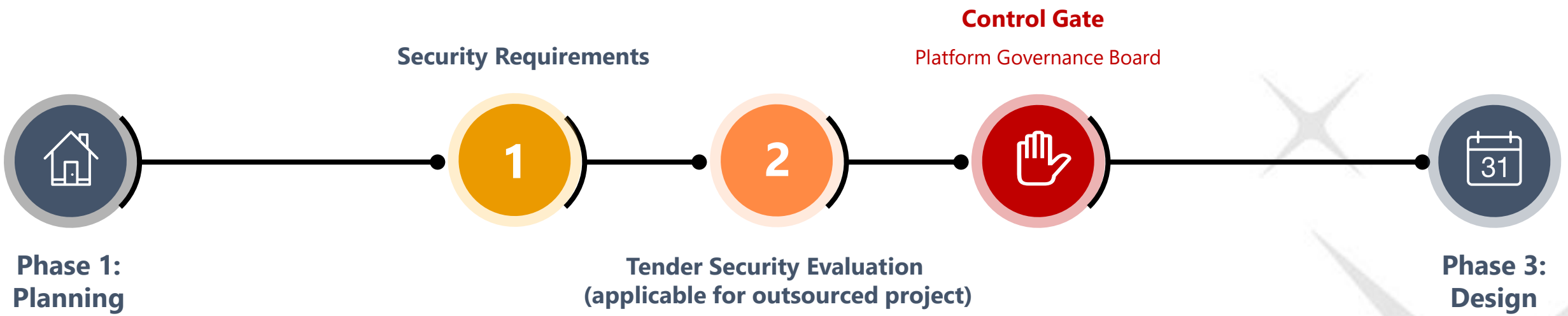
An overview of all the artefacts created at the end of **Planning** phase

	Activities	Item Name	Reference	POC	
1	Security Planning	Kick-off Deck	Being updated by Project Management	Project Management	
2	Security Classification	Security Classification	Link	ISS – CISO	
3		Availability Classification	Link	T&O	
4	Threat and Risk Assessment	TRA Report	Link	ISS – Project Advisory	

DBS

Phase 2: Requirements

Key Activities and deliverables for **Requirements** phase



Security Requirements Specification

1) Security Requirements Specification

Tender Security Evaluation

1) Outsourcing Checklist

Control Gate

1) Security Requirements
2) Outsourcing Checklist

DBS

Security Requirements

<placeholder>

Purpose

Define security requirements for the project

Artefacts

1) **Security Requirements Specification**

Reviewer

Project Manager / System Architect

References

1) **SDLC Guides and Templates**
   EASRE reference on documenting requirements under the section "Requirements"

2) **Security Catalog**
   ISS reference for relevant security controls

DBS

Tender Security Evaluation

Applicable only to outsourced projects

Purpose

Applicable for outsourced projects
Evaluate the security controls proposed by vendors to ensure that it aligns with our tender specifications

Artefacts

1) **Outsourcing Checklist**

Reviewer

ISS Project Advisory

References

Outsourcing Checklist is available from this site

Link to outsourcing process

DBS

Control Gate 2

Control Gate for **Requirements** Phase

Purpose

The purpose of this control gate is to ensure that the controls proposed by the vendors are aligned with the requirements specified in out tender specifications

Artefacts

1) **Security Requirements**
   Applicable security requirements identified from the security catalog

2) **Outsourcing Checklist**
   Applicable for outsourced projects

Gate

1) **Platform Governance Board (PGB)**
   The PGB may assign a delegate to perform this role. The delegation must be clearly documented

DBS

Summary of Key Artefacts

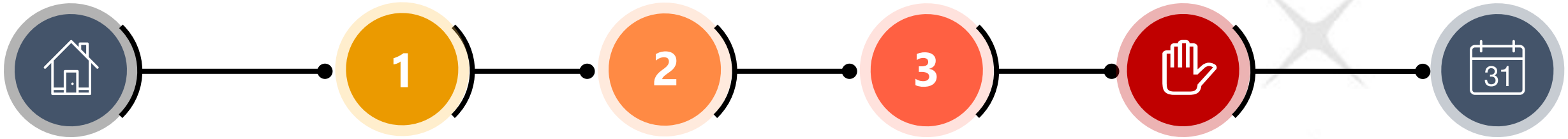
An overview of all the artefacts created at the end of **Requirements** phase

	Activities	Item Name	Reference	POC	Email
1	Security Requirements	Security Requirements	EASRE reference on documenting requirements under the section "Requirements"	Project Manager / System Architect	
2	Tender Security Evaluation	Outsourcing Checklist	Link	ISS Project Advisory	

DBS

Phase 3: Design

Key Activities for **Design** phase



Phase 2: Requirements

Threat & Risk Assessment (updated)

Control Gate

Platform Governance Board

Phase 4: Code and Build

System Security Architecture Review

1) Application Requirements Template
2) Sign-off from ISS Project Advisory

Threat & Risk Assessment

1) TRA Report (contains Risk Register)

Determine Security Controls

1) TRA Report (contains Risk Register)

Control Gate

1) Application Requirements Template
2) Sign-off from ISS Project Advisory
3) TRA Report

DBS

System Security Architecture Review

Purpose

Evaluate the security architecture of the system and propose changes or additional controls to implement, if required.

Artefacts

1) **Application Requirements Template**
   Filled up by project teams and submitted to ISS PA for review

2) **Sign-off from ISS Project Advisory**

Reviewer

1) **ISS Project Advisory (PA)**
   ISS PA will review the application requirements template from security architecture perspective

References

1) Fill up the Application Requirements Template (RIT Deck) available through this link

2) Submit a request to schedule a review through this link

DBS

Threat and Risk Assessment

Purpose

Assess the application to identify threat and risk facing the application. Thereafter , determine that the risks identified have been adequately addressed (to an acceptable tolerance level) by the proposed security controls

Artefacts

1) **TRA Report (contains Risk Register)**
   Updated to reflect the newly identified risks

Reviewer

ISS – Project Advisory
Project advisory will provide guidance and review the TRA prepared by the project teams

References

1) **Template**
   Obtain the template for the TRA report through this link

2) **Request**
   Submit a request to schedule a review through this link

DBS

Determine Security Controls

Purpose

Determine the security controls to be implemented to address the identified risks

Artefacts

1) **TRA Report (contains Risk Register)**
   Document the controls to address the identified risk

Reviewer

ISS – Project Advisory
Project advisory will provide guidance and review the TRA prepared by the project teams

References

1) **Template**
   Obtain the template for the TRA report through this link

2) **Request**
   Submit a request to schedule a review through this link

DBS

Control Gate 3

Control Gate for **Design** Phase

Purpose

The purpose of this control gate is to determine that proposed security controls are in line with ISS PA's review of the security architecture and are able to address all the risks highlighted as part of the TRA

Artefacts

1) **Application Requirements Template**
2) **Sign-off from ISS Project Advisory**
3) **TRA Report**

Gate

Platform Governance Board (PGB)
The PGB may assign a delegate to perform this role. The delegation must be clearly documented

DBS

Summary of Key Artefacts

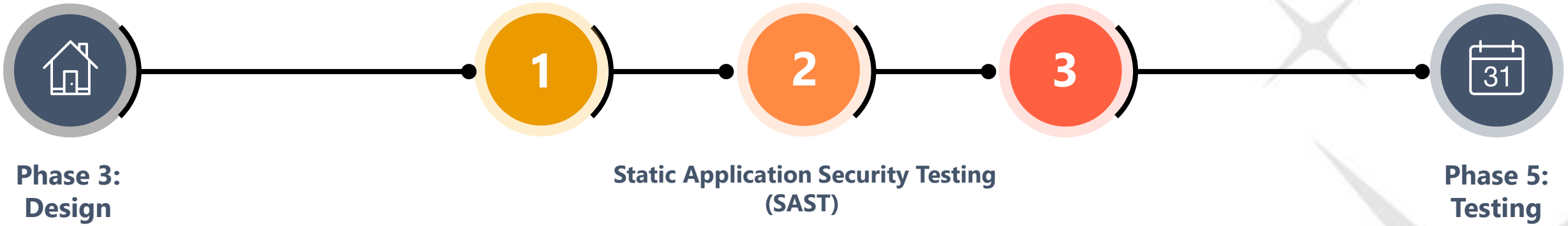
An overview of all the artefacts created at the end of **Design** phase

	Activities	Item Name	Reference	POC	Email
1	System Security Architecture Review	Application Requirements Template	Link	ISS – Project Advisory	
2		Sign-off from ISS Project Advisory	Submit a request to schedule a review through this link	ISS – Project Advisory	
3	Threat and Risk Assessment	TRA Report	Link	ISS – Project Advisory	
4	Determine Security Controls	TRA Report	Link	ISS – Project Advisory	

DBS

Phase 4: Code and Build

Key Activities for **Code and Build** phase



Source Code Review

1) Source code review report

Static Application Security Testing

1) SAST report
2) Technology MD approval for GRC

Dynamic Application Security Testing

1) DAST report
2) Technology MD approval for GRC

DBS

Source Code Review

Purpose

Analyse code for potential security vulnerabilities

Artefacts

- **Source code review report**

Reviewer

Maker-Checker within App Team

The checker will check through the code created by the maker and sign-off at the end of the review

References

- SCR Process available through this link

Static Application Security Testing

SAST

Purpose

Analyse code and binaries for potential security vulnerabilities

Artefacts

1) **SAST report**

Reviewer

Nil

This is an iterative process that allows the programmer to run the multiple scans to continuously fix the issues that were flagged.

Ideally the generated report is clean with no Medium or High issue. Otherwise, a ROR approval from the Technology MD is required

References

- Fortify playbook detailing the SAST process is available through this link

DBS

Dynamic Application Security Testing

DAST

Purpose

Analyse running program for potential security vulnerabilities

Artefacts

1) **DAST report**

2) **Technology MD approval for GRC Ticket**
   This is applicable if there are outstanding issues that could not be fixed before deployment to production

   Any "Low" issues that could not be fixed prior to go-live have to be lodged in the GRC portal

Reviewer

Nil

This is an iterative process that allows the programmer to run the multiple scans to continuously fix the issues that were flagged.

Ideally the generated report is clean with no Medium or High issue. Otherwise, a ROR approval from the Technology MD is required

References

- Fortify playbook detailing the SAST process is available through this link
- For issues that could not be remediated before go-live, submit a ticket on the GRC portal

DBS

Summary of Key Artefacts

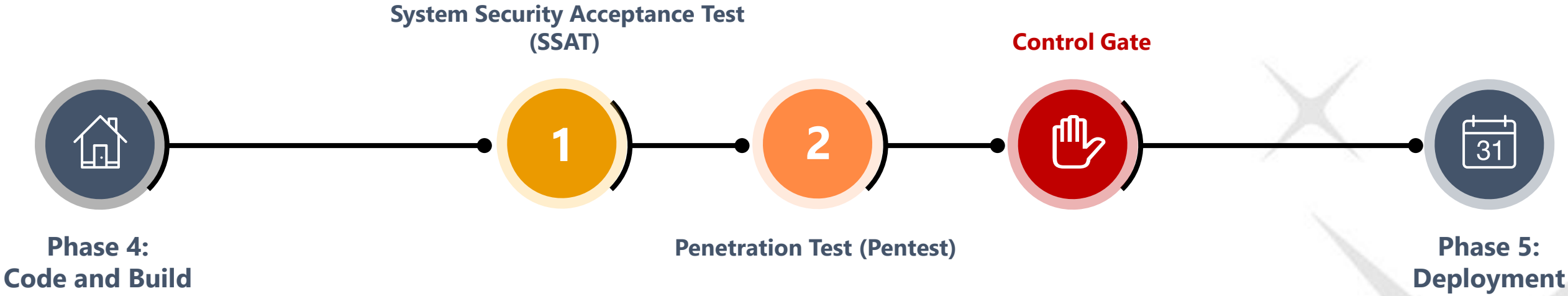
An overview of all the artefacts created at the end of **Code and Build** phase

	Activities	Item Name	Reference	POC	Email
1	Source Code Review	SCR Report	Link	ISS – App Sec	appsec@dbs.com
2		Technology MD approval for GRC Ticket	GRC portal	RMG	
3	SAST	SAST Report	Link	ISS – App Sec	appsec@dbs.com
4		Technology MD approval for GRC Ticket	GRC portal	RMG	
5	DAST	DAST Report	Link	ISS – App Sec	appsec@dbs.com
6		Technology MD approval for GRC Ticket	GRC portal	RMG	

DBS

Phase 5: Testing

Key Activities for **Testing** phase



System Security Acceptance Test

1) SSAT Report
2) SSAT Sign-off

Penetration Test

1) Pentest Report
2) Pentest Sign-off

Control Gate

1) SCR Report
2) SAST Report
3) DAST Report
4) Pentest Report
5) Pentest Sign-off
6) SSAT Report
7) SSAT Sign-off

DBS

System Security Acceptance Test

SSAT

Purpose

Analyse running program for potential security vulnerabilities

Artefacts

1) **SSAT report**
   Technology MD approval for GRC (if required)

2) **SSAT sign-off**
   Provided by ISS after fixing all pentest issues

Reviewer

ISS – Pentest

References

1) Submit Pentest request through this portal

2) For issues that could not be remediated before go-live, submit a ticket on the GRC portal

DBS

Pentest

<placeholder>

Purpose

Analyse the system for potential exploits and weaknesses that could be leveraged to compromise the system

Artefacts

1) **Pentest report**
   Technology MD approval for GRC (if required)

2) **Pentest sign-off**
   Provided by ISS after fixing all pentest issues

Reviewer

- **ISS – Pentest**

Verify that issues are fixed or lodge in the GRC portal

References

1) Submit Pentest request through this portal

2) For issues that could not be remediated before go-live, submit a ticket on the GRC portal

DBS

Control Gate 4

Control Gate for **Code & Build** and **Testing** Phase

Purpose

The purpose of this control gate is to ensure that all tests have been performed and issues have been addressed prior to deployment to production.

Artefacts

1) **SCR Report**
   Technology MD approval for GRC (if required)
2) **SAST Report**
   Technology MD approval for GRC (if required)
3) **DAST Report**
   Technology MD approval for GRC (if required)
4) **Pentest Report**
5) **Pentest Sign-off**
6) **SSAT Report**
7) **SSAT Sign-off**

Gate

Platform Governance Board (PGB)
The PGB may assign a delegate to perform this role. The delegation must be clearly documented

DBS

Summary of Key Artefacts

An overview of all the artefacts created at the end of **Testing** phase

	Activities	Item Name	Reference	POC	Email
1	SSAT	SSAT Report	Pending updates from ISS – Pentest	ISS – Pentest	
2		SSAT Sign-off	Pending updates from ISS – Pentest	ISS – Pentest	
3	Pentest	Pentest Report	Reference Link	ISS – Pentest	
4		Pentest Sign-off	Reference Link	ISS – Pentest	

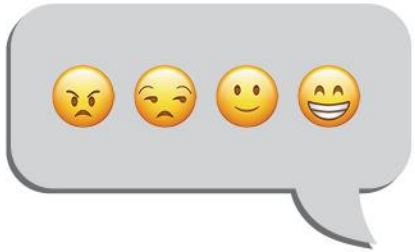
DBS

*P.S.** What would Wreckoon say?

- What is our riskiest assumption?
- What are the trade-offs?
- What could go wrong?
- Where is the data?
- What is our weakest link?
- What have we missed out?

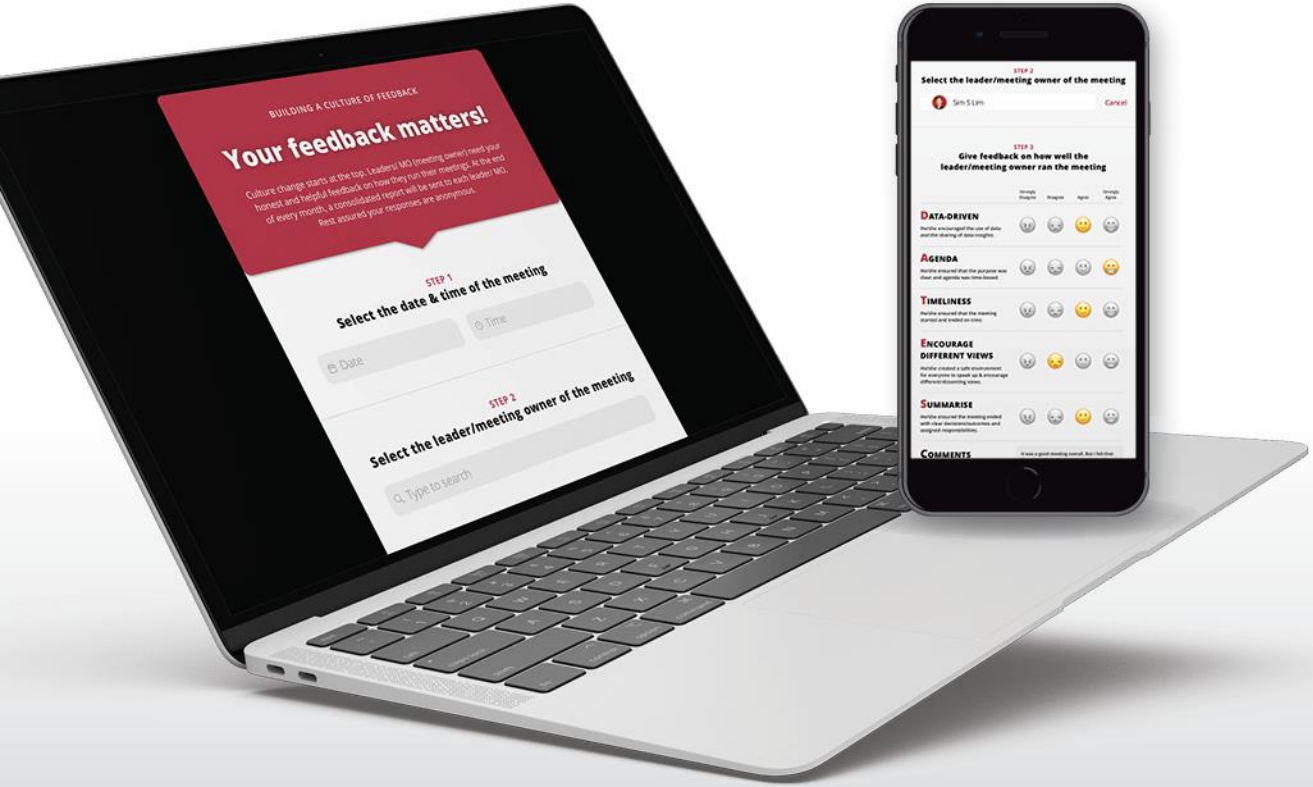
***P.S. Psychological Safety** is about creating a safe environment for everyone to speak up & encourage different/dissenting views.

At DBS, we have
MEETING MOJO



Before you leave,

Leave feedback for the manager/MO!



Laptop

Desktop Shortcut

Intranet Homepage

Mobile

Blackberry Access

Quick Access Homepage

(corporate phones only)