CYBER STANDARD DOCUMENT

SECURE BY DESIGN –
SYSTEM DEVELOPMENT

ABSTRACT:
This standard outlines the functions within the Secure By Design (SbD) process, aligned to project stages, to ensure a consistent approach to cyber security is achieved throughout a system's development. The purpose of this standard is to define an approach to ensure that all products / solutions are assured in a repeatable, structured and consistent way. This will enable security controls to be designed into solutions at an early stage, ensuring the secure delivery of solutions across policing, whilst identifying and managing risk to within risk appetite.

This standard adheres to the National Policing Community Security Policy Framework and is a suitable reference for community members, notably those who build and implement IT systems on behalf of national policing.

ISSUED	September 2023
PLANNED REVIEW DATE	September 2024
DISTRIBUTION	Community Security Policy Framework Members

STANDARD VALIDITY STATEMENT
This document is due for review on the date shown above. After this date, the document may become invalid.

Members should ensure that they are consulting the currently valid version of the documentation.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Gemma Dyson	Initial draft version	05/03/23
0.2	Gemma Dyson	Updated following NCPSWG first review	25/05/23
0.3	Tim Moorey & Emma Holmes	Re-alignment	11/07/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National approving authority	28/09/23

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021

Contents

Document Information 3
Document Location 3
Revision History 3
Approvals 3
Document References 3
Introduction 5
Owner 6
National Chief Information Security Officer (NCISO). 6
Purpose 6
Audience 7
Scope 7
Requirements 8
Feasibility, Appraise & Select, Define 8
Deliver 9
Communication approach 11
Review Cycle 11
Document Compliance Requirements 11
Equality Impact Assessment 11
Appendix A – Overview of the National Secure by Design Process 12
Appendix B – Terms and Abbreviations 16

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy Framework and associated documents sets out national policing requirements for Secure by Design.

Introduction

This standard describes the requirements to fulfil the National Community Security Policy (NCSP) System Development Policy Statement. It also describes a Secure by Design "SbD" methodology as referred to in the National Community Security Principles;

The National Community Security Principle 10: Secure by Design

Statement: The security of our information assets should never be an afterthought; security should be built in from the ground up. National systems will be assured against this principle.

Rationale: By building security into each phase of the lifecycle of a policing system, from concept to decommissioning, ensures more effective security, resulting in reduced risk, improved resilience and increased trust across the policing community.

Implications:

- All new national systems will be built and assured following a secure by design methodology.
- The development of local systems should follow secure by design principles.
- Information Asset and Risk Owners will need to be engaged throughout the system development lifecycle.

Security by design (or secure by design), sometimes abbreviated "SbD", is an industry term for a range of security practices built on one fundamental idea — that security should be built into a product/solution by design, instead of being added on later by third-party products and services.

Secure by Design as a methodology, has been selected to ensure that a repeatable, structured and consistent approach to the secure delivery of solutions across policing is achieved, as well as ensuring that risk is within risk appetite.

The Secure by Design (SbD) methodology should be aligned to the project lifecycle and internal governance of the organisation, then SbD can be followed.

Design documentation will pass through and be approved by the appropriate governance bodies within the force, organisation and/or national policing. Security Assurance will be based on documented standards and control objectives with all stages of the assurance process peer reviewed.

Building security into each phase of the lifecycle of a policing system, from concept to decommissioning, ensures more effective security, resulting in reduced risk, improved resilience and increased trust across the policing community.

This standard outlines the requirements for secure system development, the functions within the SbD process, aligned to project stages, to ensure a consistent approach to cyber security is achieved.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This standard helps organisations demonstrate compliance with the following NCSP policy statements:

System Development

- Establish a structured system development methodology that; incorporates a secure by design methodology; applies to all types of business system (including related technical infrastructure); is supported by a formal project management process; establishes specialised, segregated development environments; and involves a quality assurance process.
- Develop applications in accordance with a robust system development lifecycle, which includes applying industry good practice and incorporating information security during each stage of the lifecycle (secure by design); requirements gathering; design; acquisition (including purchase, lease and open-sourced); build; testing; implementation; and decommission.

The purpose of this standard is to define an approach to develop the maturity of assurance, ensuring that all products / solutions are assured in a repeatable, structured and consistent way. This will enable security controls to be designed into solutions at an early stage, ensuring the secure delivery of solutions across policing, whilst identifying and managing risk to within risk appetite.

This methodology should be mapped into the project lifecycle of the force or organisation it is to be used in. It is important that the Project Management Office (PMO) and third-party suppliers involved in a project are fully aware of the inputs and outputs required to progress through the project lifecycle.

The intention of this document is to provide a structured approach that can be adapted for use for all projects.

The process will:

- Provide a robust methodology by which assurance of any product / solution can be achieved.
- Allow national policing and force assurers to identify and understand security risk early in the project and support effective decision making to reduce risk.
- Ensure appropriate security controls are designed and not added.
- Give consistent and repeatable deliverables, to ensure risk is managed effectively and efficiently.
- Provide evidence for compliance and audit activities such as completion of the Security Assessment for Policing (SyAP), internal and external audits.
- Increase the maturity of assurance.

Audience

Policing Community of Trust – specifically, but not limited to, Senior Information Risk Owners (SIRO), Information Security Officers (ISO), Project Management Office (PMO) and Information Asset Owners (IAO).

This standard is aimed at:

- Information Asset Owners (IAOs) and Senior Information Risk Owners (SIROs).
- Project Management Office (PMO) and business change leads.
- Architects, system designers and engineers.
- Information & Cyber risk practitioners and managers.
- Staff across PDS and policing who are responsible for the selection, development or deployment of IT systems or applications either on behalf of national policing or at a local force level.
- Suppliers acting as service providers or developing products or services for PDS or policing.
- Auditors providing assurance services to PDS or policing.

Scope

1. The principles and methodology of this standard are the foundation for National policing IT systems, applications, or service implementations. The requirements will be applied to new and existing installations.
2. This standard is applicable to any infrastructure, system, application, or IT solution that processes or stores policing information assets.
3. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.

Requirements

The standard covers all the inputs and outputs to ensure a robust and consistent approach is taken to manage risk and assure products and services across the organisation. Several stakeholders will be required to be identified and engaged throughout this process to enable effective contribution and appropriate assignment of input and outputs at each stage.

The outputs defined may be produced by a number of stakeholders depending on the roles and governance structure of the organisation, this needs to be mapped out and responsibilities made clear. The organisation should consider producing a RACI Matrix to clearly define those responsible, accountable, informed or consulted as part of the process.

When applying this to a project, consideration should be given from the outset, on the scope of the project, ensuring it is fully understood by all stakeholders, including defining what deliverables are required. This should then be included within the project plan.

This section details the minimum requirements to implement an effective Cyber Security System Development regime to assure policing systems and information.

Reference	Minimum requirement	Control reference	Compliance Metric / Artefacts
1	**Feasibility, Appraise & Select, Define**		
1.1	Projects need to meet pre-defined information security requirements such as those described in the NCSP and associated standards, guidelines and blueprints.		Artefacts describing security requirements
1.2	Conduct Threat profiling to ensure that both generic and project specific risks are identified. Refer to the OWASP Top 10 Most Critical Web Application Security Risks and Sector specific sources such National Cyber Threat assessments, NMC threat assessments.	NIST CSF ID.RA-1 ID.RA-2	Threat assessment process in place and assessments documented. Risks identified
1.3	A Business Impact Assessment (BIA) is undertaken to assess the risks associated with the initiative. The BIA then informs decisions relating to the security requirements.	ISO 27002:2022 5.8	Business Impact Assessment conducted and accepted by Project and Information Asset Owner
1.4	System development processes need to ensure that security requirements are defined adequately, agreed security controls are developed, and security requirements are met.	NIST CSF PR.IP-2	Security Schedule in Contracts Documented processes and procedures.

Reference	Minimum requirement	Control reference	Compliance Metric / Artefacts
			Post implementation reviews.
1.5	Information security requirements need to be treated as part of business requirements and fully considered and approved.		Project artefacts
2.0	**Deliver**		
2.1	Systems are to be based on sound design principles that have security functionality built in from the outset whilst allowing for controls to be incorporated easily (System Development Life Cycle SDLC)	NIST CSF PR.IP-2 ISO 27002:2022 8.25	Documented design principles, policy and processes. Post implementation reviews.
2.2	Ensure that system development activities take place under managed change control in a segregated secure environment to minimise disruption to operational / business activity.	NIST CSF PR.DS-7	Technical architecture diagrams. Documented processes and procedures.
2.3	Software and software components acquired from external suppliers or open sources need to provide the required functionality and not compromise the security of critical or sensitive information and systems.	NIST CSF PR.DS-6	Documented processes and procedures. Evidence of testing / validation.
2.4	The asset register is updated in accordance with documented governance to reflect new assets, systems, services, software platforms and applications.	NIST CSF PR.DS-3 ID.AM-2	Documented processes and procedures. Current, up to date complete asset register.
2.5	Systems are to be designed to be able to withstand malicious attacks, and to ensure that no security weaknesses are introduced during the build process.	NIST CSF PR.IP-12	Documented designs and procedures. Vulnerability management plan. Evidence of testing / validation.
2.6	Coding vulnerabilities should be identified and remedied promptly, throughout the creation and updating of the code.	NIST CSF PR.DS-6	Documented processes and procedures. Evidence of testing / validation.
2.7	Systems should function as intended, meet agreed security requirements and ensure the security of information.	NIST CSF PR.DS-6	Documented processes and procedures. Evidence of testing / validation. Project artefacts.

Reference	Minimum requirement	Control reference	Compliance Metric / Artefacts
2.8	Avoid using real / live Personally Identifiable Information (PII) as test data. Use anonymised, randomised or pseudo anonymised data. A Data Privacy Impact Assessment (DPIA) must be completed where PII data is required to be used.	NIST CSF PR.DS-5	Documented processes and procedures. Test data examples. DPIAs Project artefacts.
2.9	Only security tested, and approved, versions of the system are permitted into the live environment.	NIST CSF PR.DS-6 PR.DS-7 ISO 27002:2022 8.19	Documented processes and procedures. Evidence of testing / validation. Project artefacts.
3.0	**Operate, Embed & Close**		
3.1	The introduction of new systems or applications is managed in accordance with change management controls in order to minimise the risk of disruption to operational / live environments.	NIST CSF PR.IP-3	Documented change management processes and procedures. Risk assessments. Minutes / notes from Change Boards.
3.2	Throughout the lifecycle business assets are formally managed throughout removal, transfers, and disposal. This can be achieved through regular management reviews such as security working groups.	NIST CSF PR.DS-3	Documented processes and procedures. Records of processes.
3.3	Assets are disposed of according to records management & information security policies.	NIST CSF PR.IP-6	Documented processes and procedures. Asset certificates of destruction.

Communication approach

This standard will be communicated as follows:

1. Internal peer review by the members of the National Cyber Policy SWG (External), which includes PDS and representatives from participating forces.

2. Presentation to the NCPSB for approval.

3. Formal publication and external distribution to PDS community, police forces and associated bodies.

This standard should be distributed within IT and project teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / Security Management Forum / Information Management. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.

This standard should be mapped to a project lifecycle and internal governance prior to adoption. Following this, it should be provided to the Information Assurance communities and PMO's and should also be shared with procurement & commercial leads to ensure this is built into procurement activities.

Measurables generated by adopting this standard can also form part of regular Cyber management reporting and audit evidencing.

Review Cycle

This Policy will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the policy continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

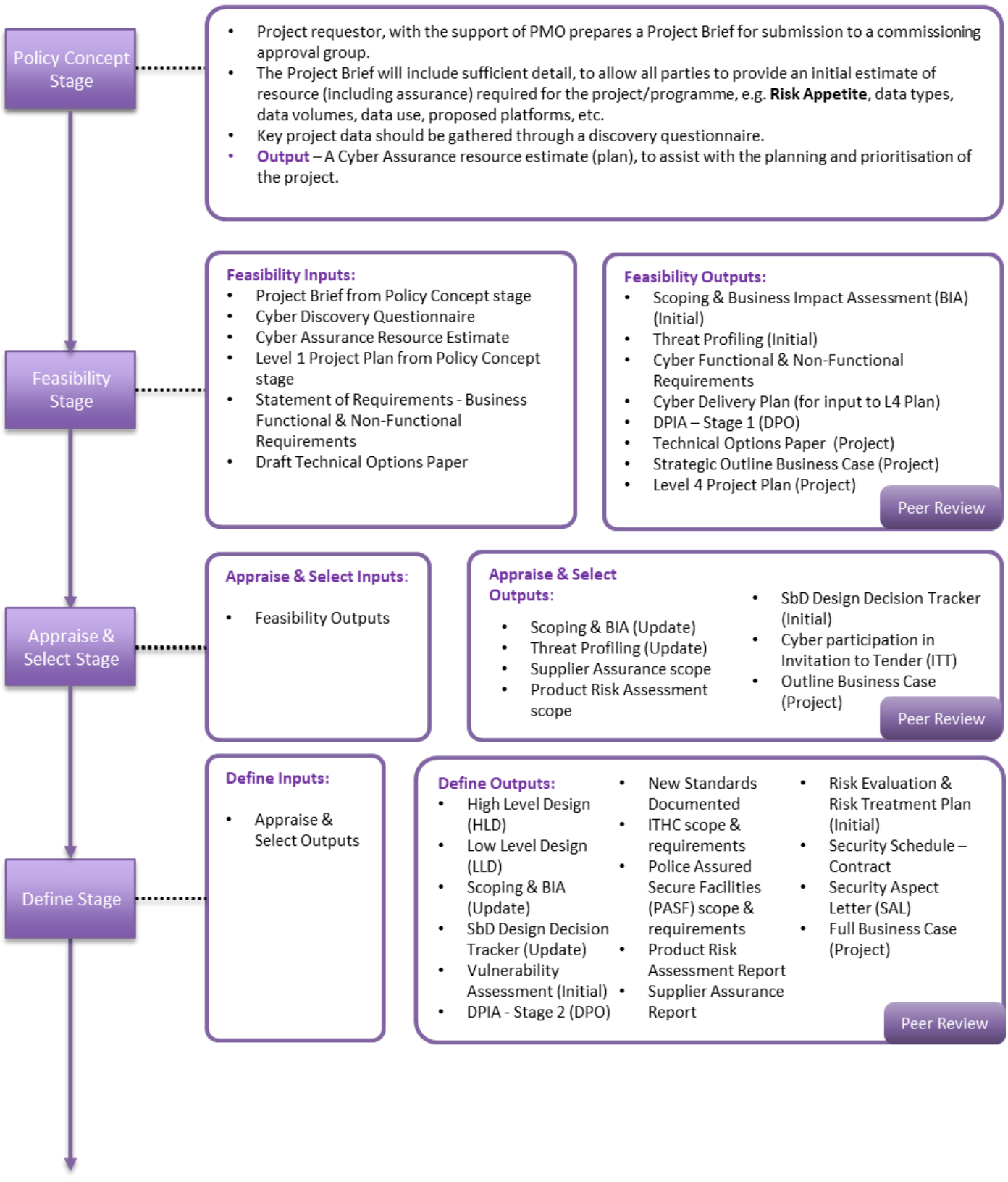
Appendix A – Overview of the National Secure by Design Process

Project Lifecycle Stages	Description
Policy Concept	The stage name is derived from many government projects started as a result of a policy decision. It's defined as the stage where the project requestor will work with project management office (PMO) to create a Project Brief, to request project support.
Feasibility	This stage is to begin to understand what is possible, how long it might take and how much it might cost. The project will gather requirements and produce an Outline Business Case and a High-Level Plan during this stage.
Appraise & Select	This is the stage where we consider what we might want to buy or build in terms of service(s) and/or product(s) to meet the requirements defined earlier. An Invitation To Tender is produced, if required.
Define	During this stage any Invitation To Tender will be published and the service/product suppliers selected. By the end of this stage, the project will have produced the High-Level Design(s) and a Full Business Case.
Deliver	This is where the solution is built and tested. If this is successful, the project will finalise the production of a Low-Level Design and a draft closure plan.
Operate, Embed & Close	The project operates the solution and embeds it into the business, ironing out any issues and getting it ready to hand over to the business to run.
Operations	If everything has gone to plan, the solution will now be in full operational service, the project will have closed and day to day operations will be managed by a Business-As-Usual Team.

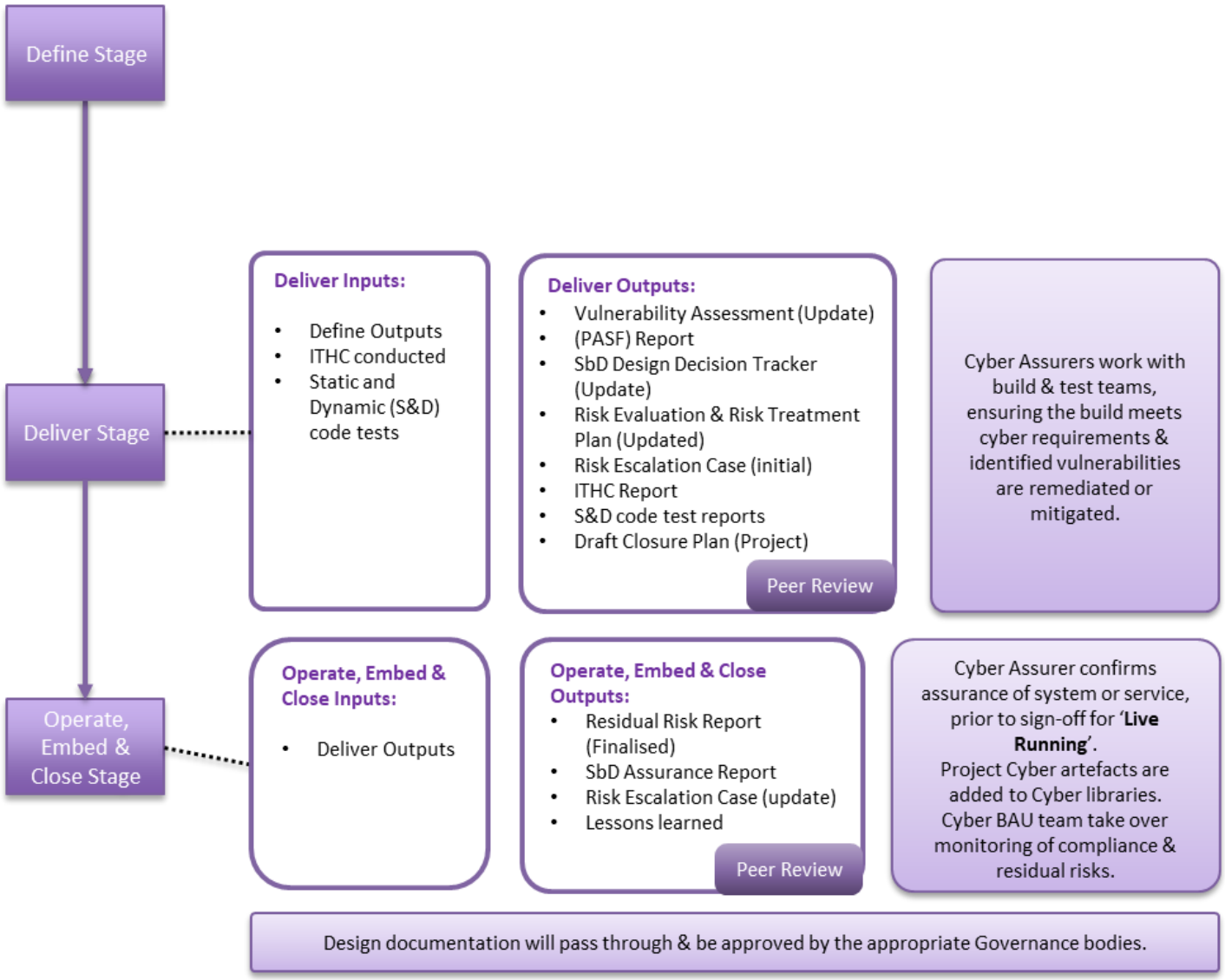
At each stage of the project lifecycle, numerous inputs are required to allow for the security assessment to begin and outputs (deliverables) to be created. It is important to note that without the appropriate documentation from the project and/or supplier, the outputs cannot be achieved, and assurance will be limited or not gained.

Many security controls are applied by following this process, which ensures that risks are managed effectively and efficiently and are mitigated throughout the process rather than at the end.

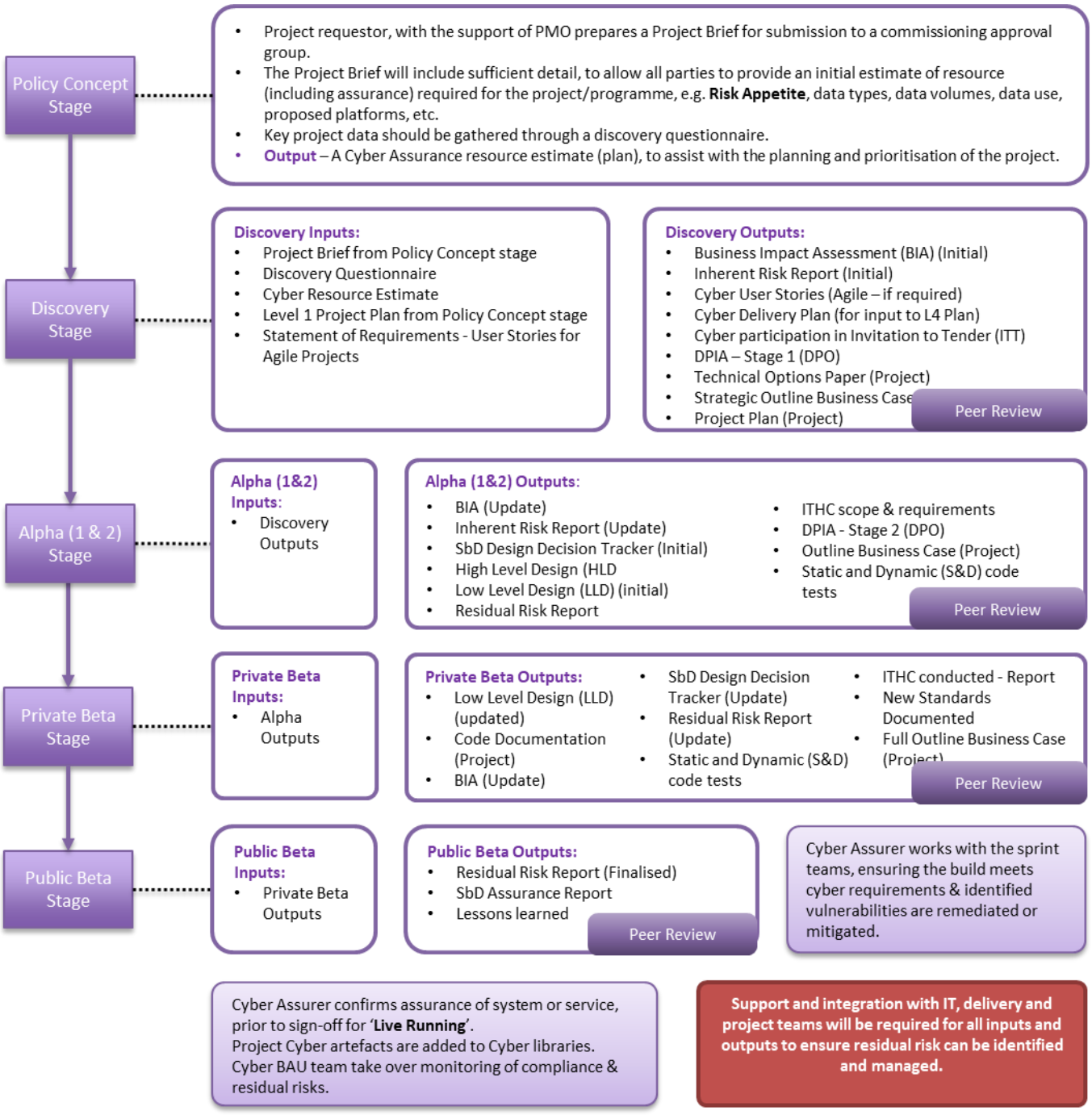
SbD Assurance Waterfall Process



SbD Assurance Waterfall Process Continued



SbD Assurance Agile Process



Appendix B – Terms and Abbreviations

Term	Abbreviation	Brief explanation
Business Impact Assessment	BIA	An assessment of the impact to compromise of confidentiality, integrity, and availability of information assets.
Controls		Mitigations or countermeasures to vulnerabilities. These can be technical (a firewall), administrative (policies and procedures) or physical (security guard).
Data Protection Impact Assessment	DPIA	A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
Design Decision Tracker		This document tracks deviations from a standard and the design decisions made.
High Level Design	HLD	High-level design (HLD) explains the architecture that would be used to develop a system.
High Level Technical Architecture Design	HLTAD	The architecture diagram provides an overview of an entire system, identifying the main components that would be developed for the product and their interfaces.
Inherent risk		Risk before any controls are applied.
IT Health Check	ITHC	An ITHC is a series of controlled ethical hacking tests and actions designed to deliberately identify and expose security vulnerabilities that might be present.
Low-Level Design	LLD	Low Level Design (LLD) is specifying the HLD and describes the actual logic for the entire components of the solution. Detailed Network Security functional diagrams with all the relations and methods among all logic come under the Low-level design. Technical specifications are included with references to the HLD. LLD explains all the functional parts of the solution.
Police Approved Secure Facility	PASF	A specific assessment of physical security of a facility processing policing data.
Residual Risk		Risk after controls are in place.
Security Aspects Letter	SAL	A Security Aspects Letter is a contractual document that establishes the security principles of a supplier or third party processing data.
Target Risk		Risk target after further controls are put in place.