

Security and Privacy by Design and Assurance Process Manual

Cyber Secure By Design



October 2022

| | |
|-------------------------|-----------------|
| Author | Kally Mabe |
| Version Number | 1.0 |
| Status | Draft |
| Security Classification | C2 – Restricted |
| Date | 05 October 2022 |

Document History

| Version | Date | Change Summary |
|-----------|------|-----------------|
| Version 2 | 2.0 | Added workflows |
| Version 3 | 3.0 | Grammar changes |
| | | |

Approvers

| Name | Role | Department | Date | Signature |
|------------|-------------------------|----------------------------|----------|---|
| Kally Mabe | Senior Specialist – 2IC | VSA Cyber - SecureByDesign | 15/10/22 |  |
| Kally Mabe | Line Manager | VSA Cyber - SecureByDesign | 15/10/22 | <div>DocuSigned by:</div>  <div>95402D6F2D5C42C...</div> |

Contents

| | |
|--|----|
| Contents | 3 |
| 1 Controls and Deliverables required for compliance | 4 |
| 1.1 Purpose of SPDA | 4 |
| 1.2 Mandate of SPDA | 5 |
| 1.3 Scope of applicability | 5 |
| 1.4 SPDA High level Process Overview | 5 |
| 1.4.1 Entry and exit conditions | 6 |
| 1.4.2 SPDA in Waterfall | 6 |
| 1.4.3 SPDA in Agile | 7 |
| 1.5 SPDA Gates (Stages or Phases) | 8 |
| 1.5.1 SPDA key security focus areas – Baseline Security Requirements | 8 |
| 1.5.2 Demand (Requirements and Information) | 8 |
| 1.5.3 Due Diligence (Governance, Regulatory and Compliance) | 9 |
| 1.5.4 Design (Architecture & Stakeholder Alignment) | 9 |
| 1.5.5 Development (Requirements and Testing) | 9 |
| 1.5.6 Deployment (Operational Requirements) | 9 |
| 1.5.7 Delivery (Technology Security Verification and Monitoring) | 9 |
| 1.5.8 Defend (Monitor, Maintenance and Awareness) | 9 |
| 1.5.9 Decommissioning (End of Live Security Management) | 9 |
| 2 Security Attributes relating protection of Information | 9 |
| 3 SPDA Knowledge Base and tools | 10 |
| 4 Budgetary Provisions | 11 |
| 5 Evidence and reporting | 11 |
| 6 Exception & Risk Acceptance | 11 |
| 7 Process violation | 12 |
| 8 Review of this process | 12 |

1 Controls and Deliverables required for compliance

1.1 Purpose of SPDA

SPDA is a demonstrable end-to-end process methodology that consists of a series of security, privacy, and business risk steps, typically within a [waterfall](#) or [agile](#) product or service development lifecycle, for:

1. **Identifying potential privacy, business, and security risks** for new products, services, and operations (“product”) **and identifying controls** to minimize, mitigate or remove those privacy, business, and security risks (at Idea & Concept stages);
2. **Designing and implementing the identified controls** into the product (at Design & Build stages);
3. Assuring that privacy, business, and security controls have been implemented before the product goes “live” and product complies with Vodacom Security and Privacy requirements and applicable laws (at Test & Go-Live stages);
4. **Addressing security and privacy risks arising from changes to existing live products** that impact the processing of personal data (In-Life); and
5. **Ensuring security and privacy risks are addressed when decommissioning** these products (Decommissioning).

SPDA incorporates two concepts:

1. **Security and Privacy by Design:** This encompasses those elements of the process that identify privacy, business and security threats and risks, as well as designs and implements privacy, business, and security safeguarding controls into products from the beginning, not as an afterthought.
2. **Security and Privacy Assurance:** These are the steps required to confirm that the products and services have been built in such a way as to conform to that privacy, business, and security controls.

In addition to its main purpose, SPDA provides the following benefits:

1. **Accountability:** SPDA defines key activities and decision points with related responsibilities to ensure business takes informed decisions
2. **Consistency, speed, and certainty:** Standardized process steps ensure high-quality outputs, speed of execution, and consistent implementation of Vodacom policy
3. **Operational efficiency:** Reduction of overlapping work by integrating Security and Privacy activities. Supports planning and execution of plans and demand management
4. **Cost efficiency:** Avoiding unnecessary costs, as the cost of mitigating potential security and privacy challenges increases later in the development security or privacy concerns are addressed
5. **Demonstrability:** Ability to demonstrate to Vodacom senior management, data protection authorities, customers, and other key stakeholders that Vodacom has in place effective processes to ensure our products and services comply with Vodacom’s internal privacy and security policies and legal and regulatory obligations
6. **Continuous improvement:** Standardised processes provide visibility into quality, productivity, cost, and timeliness for improving the process and raising the maturity of security and privacy risk management
7. **Low barrier of entry for new resources and knowledge transfer:** Standardised processes improve communication and understanding, enable pushing work to lower levels of expertise, reduction of key personnel dependencies, and effective knowledge transfer for new employees
8. **Reporting:** Same process and methodology across the organization enables comparable reporting, group-wide management of compliance and risk management activities, and continuous improvement

1.2 Mandate of SPDA

Policy Alignment: SPDA and the security leg, Secure by Design, are required by the Cyber & Information Security Global Policy [Reference 1] and the Secure System Development Lifecycle policy.

Law: SPDA is also required or pre-supposed by data protection laws, for example, the POPIA. POPIA requires Vodacom to implement technical and organizational measures to ensure and to be able to demonstrate that the processing of Personal Information is performed in accordance with the law. SPDA satisfies the POPIA requirements as it applies where Responsible Parties process Personal Information in South Africa, regardless of where the Responsible Party is situated. It applies to both natural and juristic persons, customers, clients, employees and direct contractors, and suppliers.

1.3 Scope of applicability

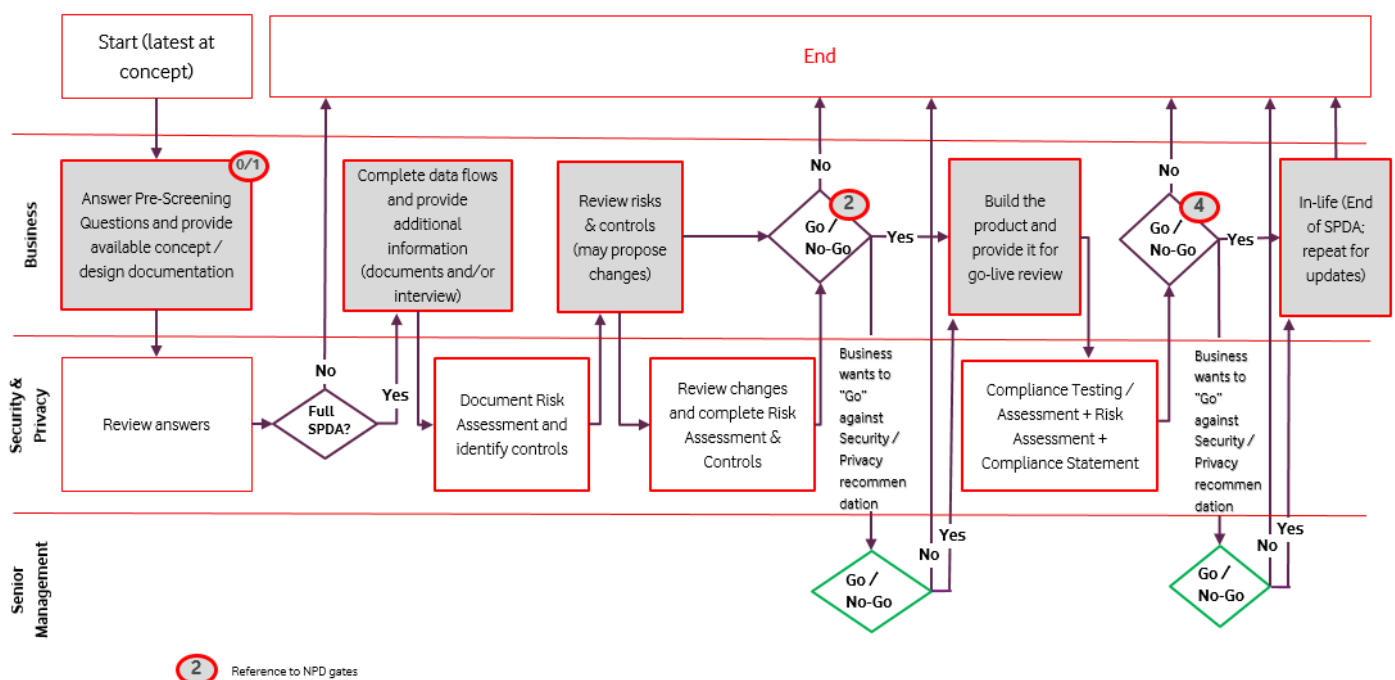
SPDA applies to:

- 1. All Vodacom:** SPDA applies across all Vodacom entities
- 2. All new products, services, or operations:** SPDA applies to the development, launch, and in-life changes of all Vodacom products, services, and operations. This includes, for example, connectivity services, IoT products, online services, mobile applications, marketing and other CVM collaborations where personal data is processed, software or a hardware product, research activity, analytics, IT process, operation, related office, and front office processes, or even a commercial collaboration contract, M&A, sourcing, outsourcing or a partnership;
- 3. All Personal Data:** The personal data in question may relate to consumers, employees, external workforce, and other personal data collected or processed by or within Vodacom products, services, and operations (“product”).

1.4 SPDA High-level Process Overview

The SPDA process is set out as a series of key phases with required steps and decision points that should be integrated into existing product development processes, such as NPD, or which should be introduced where there are either gaps in existing processes or there are no existing processes.

Process for completing the SPDA documentation



1.4.1 Entry and exit conditions

The entry conditions for SPDA are:

1. New Product, Service, and Operations;
2. Significant update(s) to an existing Product, Service, or Operation that has an impact on the way personal data is processed, for example:
 1. Design and functionality of the product or service
 2. The types of personal data collected
 3. How the personal data are collected
 4. How the personal data are to be used
 5. Where the personal data are to be stored
 6. The suppliers or third parties involved in the delivery (for example a change of, or inclusion of a new, supplier)
3. Decommissioning of a Product, Service, and Operations
4. Incidents, threats, new vulnerabilities, changes in laws, regulations, or other such changes in the Vodacom business environment lead to a need to verify compliance

The exit condition for SPDA is:

1. Successful privacy, business, and security assessment before Go-Live; and/or
2. Risk Acceptance at the right level of seniority appropriate to the risk exposure

Exclusions: Subject to Local Market decisions, the following types of situations are not subject to SPDA:

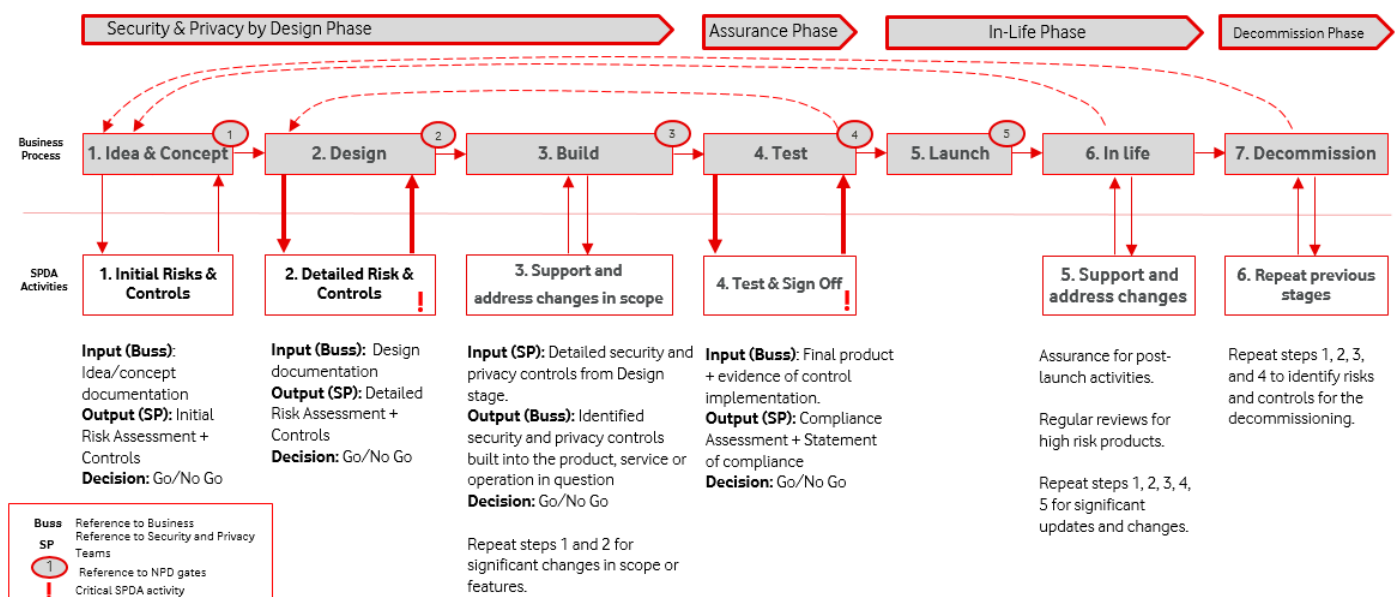
1. Marketing campaigns (e.g. print or online. NOTE, however, that e.g. an agreement to enter into marketing collaboration with a social media provider which includes e.g. sharing of personal data is always subject to SPDA);
2. Minor changes without impact on the processing of personal data in previously assessed objects (e.g. non-functional changes);
3. Components supporting the product in question (e.g. billing or customer care), to the extent such components have been recently reviewed and are subject to other assurance activities (e.g. High-Risk Processing Assessments).

NOTE, however, that such an exclusion is only permissible to the extent detailed requirements have been defined for such excluded activities, and the case at hand falls within such detailed requirements.

At a high level the SPDA consists of the following process steps and activities (for Waterfall & Agile):

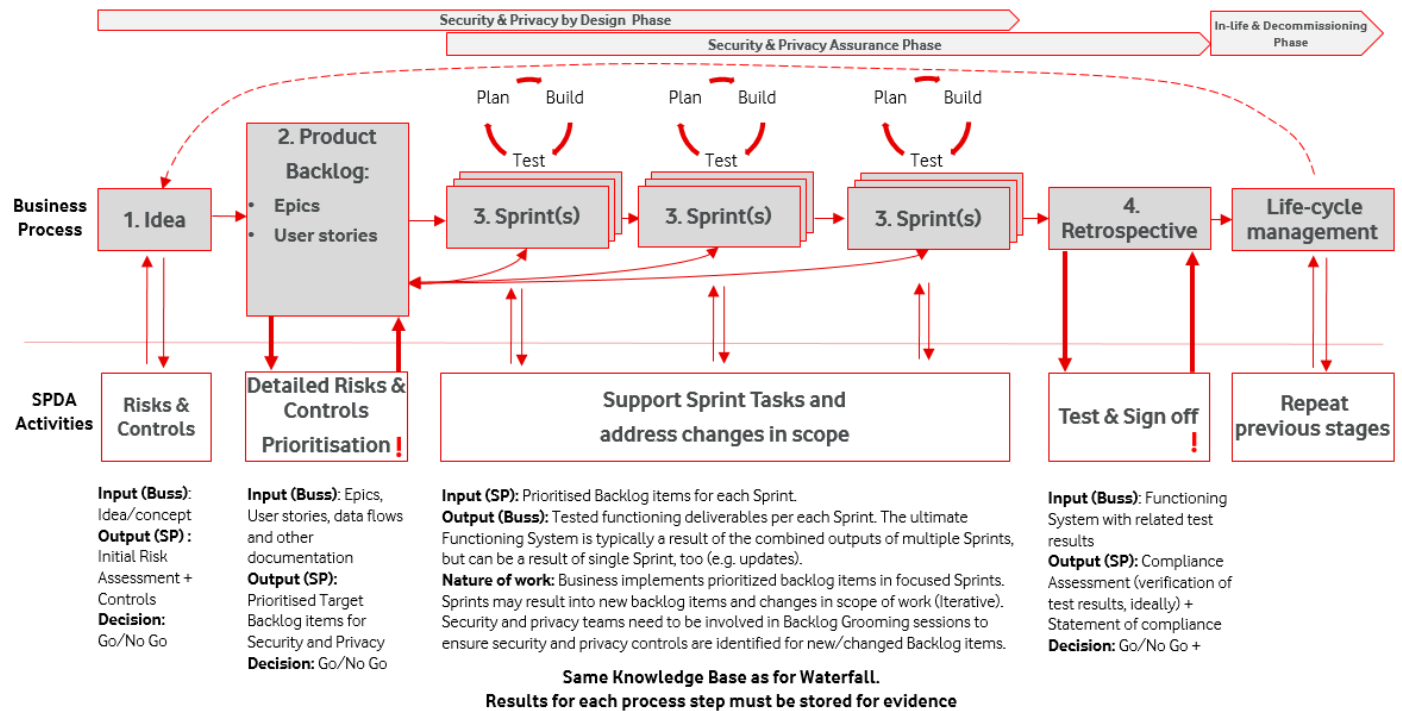
1.4.2 SPDA in Waterfall

Security and Privacy by Design & Assurance in Waterfall



1.4.3 SPDA in Agile

Security and Privacy by Design & Assurance in Agile



1.5 SPDA Gates (Stages or Phases)

SPDA covers 8 typical SDLC stages of phases by applying the **Cyber Security Baseline (CSB) requirements** as applicable:

| CSB Domain Alignment | |
|---------------------------------|---|
| Cyber Defence | ✓ |
| Identity & Access Management | ✓ |
| Information Protection | ✓ |
| Network Security | ✓ |
| People Security | ✓ |
| Security Hygiene & Essentials | ✓ |
| Software Development | ✓ |
| Supplier & Third Party | ✓ |
| VC Products & Services Security | ✓ |

1.5.1 SPDA key security focus areas – Baseline Security Requirements

The Secure by Design aspect of the SPDA is performed using the Baseline Security Requirements template. The key security areas, which we aim to understand, manage, assess and monitor, as outlined in the Baseline



Baseline Security
Requirements.xlsx

Security Requirements template are:

- Stakeholder and Project Information
- Security Hygiene and Essentials
- User and Account Management
- Data Protection
- Logging and Monitoring
- Data Protection (C3/C4)
- API Design
- Cloud Computing
- Supplier and 3rd Party
- Web Application Security
- Mobile Security
- VOIP
- CPE
- Technical Assurance

1.5.2 Demand (Requirements and Information)

The demand process is always associated with a requirement and all requirements are subject to a risk and security assessment. Risk assessments help to clarify the requirement as well as to understand the associated security posture. All demand needs to be formally logged in JIRA. Logging an SPDA demand request, through JIRA will initiate assessments by Cyber Security, Vodacom Privacy, and Corporate Risk which collectively will facilitate the completion of the SPDA process and approval.

Documentation such as a “Business Requirements” or in case of compliance, Cyber Security Baseline (CSB) controls is verified by use of the BSR and other assessment templates that are previously approved and guarantee the intent or this requirement can be defined by security frameworks like the Payment Card Industry Data Security Standard (PCI DSS) or ISO/IEC standards that are applicable. Based on the outcome of the risk assessment, the Risk Management areas such as Compliance, Cyber Security, and/or Corporate Security can advise or proceed accordingly.

1.5.3 Due Diligence (Governance, Regulatory, and Compliance)

Due Diligence is the process to verify governance, regulation, and compliance. During this stage/phase, Vodacom makes use of a procedure and tools that are aligned with Supply Chain and Privacy requirements, the tool must provide the Privacy team and Cyber Security team to assess and manage cyber requirements when third parties are involved.

1.5.4 Design (Architecture & Stakeholder Alignment)

Any system/solution requires the input and engagement of various stakeholders, namely Cyber Security Risk Management covering Assets, Infrastructure, Networks, Business, Operations, and Wireless (RAINBOW).

Any SPDA Request should be submitted with an accompanying formally documented architecture. The Architecture should be documented using the HLD template created by the Vodacom South Africa IT Architecture team. Refer to [HLD Template V1.1.docx \(sharepoint.com\)](#)

From an Architecture review perspective, the Vodafone Baseline Security Requirements template in the latest version available must be completed for higher-risk projects and updated by the project team for review by Secure by Design.

1.5.5 Development (Requirements and Testing)

Developing and testing with security in mind requires a specific mindset around best security practices as defined in frameworks like the Open Web Application Security Project (OWASP). Processes like manual and/or automated Code Reviews focused testing (functional, stress, security, etc.), and automated security scans (at least on the pre-production environment) for both infrastructure and applications are very important.

1.5.6 Deployment (Operational Requirements)

SPDA addresses the operational deployment aspect of products/solutions through CSB requirements which ensures proper hardening, segregation of duties, change control, etc. Other aspects for example Service Level Agreements (SLA), logging, and monitoring are all part of good, clean security processes.

1.5.7 Delivery (Technology Security Verification and Monitoring)

All the requirements before and after a project/system/solution move into a production environment need to be verified against the necessary security CSB requirements.

1.5.8 Defend (Monitor, Maintenance, and Awareness)

Once live, a security maintenance and monitoring program is required in line with the demand management processes which include incident response, change management, vulnerability management, event logging, monitoring, etc.

1.5.9 Decommissioning (End of Live Security Management)

In cases where a system is required to be decommissioned, a decommissioning process must be applied to apply using a formal security destruction/phase-out project or process.

2 Security Attributes relating protection of Information

When performing an SPDA the SPDA practitioner should consider and recommend how different attributes of information should be protected depending on the type and sensitivity of the information and the specific control requirements outlined in Vodafone Policies and standards, including:

- Confidentiality: to prevent unauthorized disclosure of sensitive information
- Integrity: to prevent the integrity of critical information from being compromised
- Availability: to prevent critical information from becoming unavailable.

3 SPDA Knowledge Base and tools

Knowledge Base: SPDA Knowledge Base documents the pre-defined controls and design patterns to be communicated to the business. To ensure consistent deployment of Vodacom's relevant Security and Privacy Policies, the Cyber Security Officer (CSO), Privacy Officer (PO), Business Risk Office (BR), Security Architecture Officer (SAO), and Group Risk and Compliance Officer (GRC) roles should investigate the SPDA Knowledge Base to identify controls and to adapt such controls to the case at hand. In case pre-defined controls do not apply to the case at hand, the CSO, PO, BR, SA, or GRC should apply his/her expertise or, in case of a more junior assessor, reach out to the responsible cyber security/privacy/business risk person to define appropriate controls for the project or solution context. Such controls, if similar situations are likely to recur, should be integrated into the SPDA knowledge base for later use.

The knowledge base for identifying privacy risks and defining controls in brief:

| # | Document Title | Location |
|----|--|--|
| 1 | Cyber & Information Security Global Policy | Global Cyber Security Link |
| 2 | Tier 3 Standard: Secure Agile Development | Global Cyber Security Link |
| 3 | Information Security Classification and Protection Detailed Requirements | Global Cyber Security Link |
| 4 | Cyber Security Testing Detailed Requirements | Global Cyber Security Link |
| 5 | Tier 3 Standard: System & Service Security Zoning | Global Cyber Security Link |
| 6 | Secure System Management and Protection Detailed Requirements | Global Cyber Security Link |
| 7 | Supplier Information Security Detailed Requirements | Global Cyber Security Link |
| 8 | Security Risk, Control & Assurance Framework | Global Cyber Security Link |
| 9 | Tier 3 Standard: Information Sanitisation and Disposal | Global Cyber Security Link |
| 10 | Records Management and Data Retention Global Policy | Group Corporate Security Link |
| 11 | Secure System Development Lifecycle | Group Corporate Security Link |
| 12 | SPDA How to Guideline | Vodacom Cyber Secure by Design |

| | | |
|----|---|---|
| | | |
| 13 | Policy Dispensation and Security Risk Assessment Requirements | <u>PD and SRA Requirements - Vodacom 2021-11-17.pptx (sharepoint.com)</u> |

4 Budgetary Provisions

Due to the increasingly high number of new products and services in Vodacom, and considering the limited resource capacity in security, privacy, and business risk teams to accommodate the increasing demand, Product and Business owners are advised to allocate a budget for security and privacy compliance assessments, as well as security testing (e.g. penetration test) or design creation activities, to ensure that security, privacy, and business risk resources are assigned to the project early on in the development lifecycle.

Security, Privacy, and Business Risk officers will in most cases advise on more specific budgetary requirements and any other provisions at the Idea/Concept phase, or early in the Design Phase. Having the budget available promptly would help prevent delays to the compliance assessment completion and therefore product/service launch.

5 Evidence and reporting

Evidence relating to inputs and outputs of SPDA process steps must be stored in a repository for later use. The recorded evidence must answer questions such as “what was the business instructed to do?”, “who was involved in the assessment?”, “on what information was the assessment based?” or “who took the decision and based on what recommendations?”. Each team, Technology Security, Business Risk, and Privacy are responsible for storing their respective parts in a central repository within their team. The evidence stored and made available for later use must include:

1. Product and business owners
2. Participants in the review and signoffs
3. Data flow mapping and detailed list of data attributes, their purpose of use, and identified retention schedules for the data in question
4. Risk Assessment and identified security and privacy controls
5. The results of the compliance assessment, including recommendations
6. Decisions, escalations, and their outcomes
7. Whether or not the product includes High-Risk Processing, and if yes, an audit cycle must be defined

For Vodacom South Africa SPDA Demand and assessments are stored and managed on JIRA and OneTrust.

6 Exception & Risk Acceptance

Where the Product Owner fails to implement the privacy & security controls required by the Cyber Security Officer, Business Risk Officer, and Privacy Officer, or despite implementing the required privacy & security controls, the residual privacy risk remains high on the product, a risk acceptance process shall be triggered by the Group Privacy and/or Cyber Security Officer and/or Business Risk Officer and/or Group Risk and Compliance Officers to escalate the risk decisions to next level of appropriate seniority. For more information regarding the exceptions and risk acceptance, please refer to [PD and SRA Requirements - Vodacom 2021-11-17.pptx \(sharepoint.com\)](#)

7 Process violation

1. Anyone found to violate this process or standards defined in this process, in the implementation of systems or services, may be subjected to HR disciplinary actions per HR disciplinary policies and procedures.
2. Non-compliance to any of the requirements in this process or referenced documents must have an approved Policy Dispensation or Cyber Security Risk Acceptance completed. Refer to [PD and SRA Requirements - Vodacom 2021-11-17.pptx \(sharepoint.com\)](#)

8 Review of this process

This process shall be reviewed in a period not exceeding one year or earlier as recommended by Vodacom Management and/or forces from Technology changes.