



Doc No. V5	SPDA How to Guideline			Rev. 2
Applicable areas of business: Vodacom SA		Responsible Division Technology Security (Darshan Lakha -EHOD)		
Approval	Name	Job Title/ Role	Signature	Date
Content Owner	Kally Mabe	Senior CSO – 2IC		15/10/2022
Approved by	Christopher Knox	Manager: Cyber Security	 DocuSigned by: 95402D6F2D5C42C...	15/10/2022

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA Process Document

Revision: 1

Owner: Chris Knox
Page 0 of 95



CONTENT

1. SPDA Procedure.....	2
2. JIRA: Viewing, Moving Tickets along the process, and Closing Tickets in JIRA	7
3. Initial Qualifying Questionnaire	12
4. OneTrust: Launch SPDA Assessment BSR	18
5. OneTrust: Cyber Security Assessment – Baseline Security Requirement.....	24
6. OneTrust: How to Raise a Risk	69
7. Decommissioning	83
8. OneTrust: Launch Decommissioning Assessment.....	85
9. OneTrust: Cyber Security Assessment - Decommissioning	87
10. Risk Definition and Prioritisation.....	91
11. Definitions:.....	92
12. Roles and Responsibilities.....	93
13. Supporting documents / Policies.....	94
14. Document history	94

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe

Page 1 of 95



1. SPDA Procedure

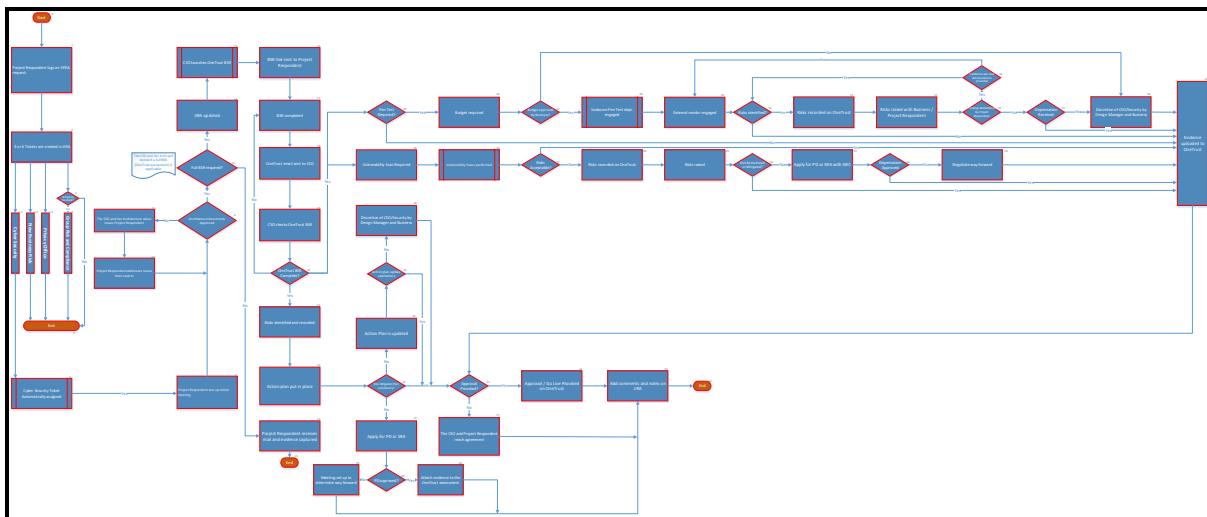


Figure 1- Cyber Security SPDA Process

- 1.1 An SPDA is initiated by an individual logging a request in JIRA, known as the Project Respondent, as per JIRA naming convention. The request includes either logging a ‘Feature’ in JIRA and answering the mandatory questions for PI initiatives, or by completing the Initial Qualifying Questionnaire Template in Confluence for non-PI initiatives
 - 1.2 For PI initiatives, the system automatically creates 3 tickets one on each of the 3 areas boards (Cyber Security, Privacy, and New Business Risk). Alternately, for non-PI initiatives, 3 tickets are created by the Project Respondent, via the Initial Qualifying Questionnaire, one on each of the 3 areas boards (Cyber Security, Privacy, and New Business Risk)
 - 1.2.1 The Cyber Security Ticket is created in JIRA
 - 1.2.2 The New Business Risk Ticket is created in JIRA
 - 1.2.3 The Privacy ticket is created in JIRA
 - 1.3 If a third-party assessment is required to be completed, then
 - 1.4 A fourth ticket is created by the Project Respondent on the Group Risk and Compliance Board
 - 1.5 For purposes of this document, we will only detail the Cyber Security ticket further, and thus, the other processes that are mentioned continue further in their respective area’s documents, however, will not be detailed further in this document
 - 1.6 The Cyber Security tickets are automatically assigned to the relevant CSO when they are created in JIRA. Each Business Unit (BU) has a dedicated CSO from the Cyber Secure by Design team. For a full list of CSO’s per BU, and further information regarding the SPDA process, please visit our [Secure By Design Confluence Page](#)
 - 1.7 The Project Respondent then arranges a meeting with the Application Technical Team, the Cyber Security Team, and the Security Architecture Team to review the design documents and answers to the Initial Qualifying Questionnaire. During the meeting, the Project Respondent/Business will provide details, share designs, outline the system, and detail the data flow. The CSO and Security Architecture try to understand which security controls apply to that specific design

The following documents, were applicable, are required to be sent to the CSO before the meeting:

- High-Level Design

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guidelines

ED OR REF
Revision: 2

Owner: Kally Mabe
Page 2 of 95



- Low-Level Design
- Dataflow Diagrams
- Comms Matrix
- User Story Diagrams

Note: Should these documents not be available at the time of logging the 'Feature' / tickets, the tickets will be moved to a suspense stage of the process. The ticket will remain in this suspended state until the relevant documents/information has been provided

- 1.8 Have the Architecture Documents been approved by the Security Architecture team and the CSO at the meeting set up in 1.10?
- 1.9 Where the solution design is missing or has not included important security-related requirements the CSO will raise issues or concerns to be addressed before the architecture document is signed off. If the Security Architecture Team discovers risks or possible changes, they will notify the Project Respondent in the meeting, via comments in JIRA and update the architecture document on the issues sections. If the issues raised during the walkthrough aren't addressed a form risk will be raised against the application. The comments and approvals are captured in JIRA on the Security Architecture Kanban board. (Where Design Documents are not applicable, a Dataflow Diagram and User Story Diagram will be required)
- 1.10 The Project Respondent addresses the risks raised and reverts to the CSO and Security Architecture and the process moves back to 1.11
- 1.11 Depending on the type of change request or development, criticality rating, data types, and context, the CSO and Security Architecture will also determine if a full BSR assessment is required to be completed by the Project Respondent. The 'Critical' and 'High' criticality ratings generally require a full BSR to be completed, and the 'Medium' and 'Low' criticality ratings are managed in JIRA
- 1.12 If no BSR assessment is required to be completed, the CSO will email the Project Respondent with feedback and update the JIRA ticket accordingly. Approval from Cyber Security may be provided, with or without conditions to be met by a specific date. Projects which are determined to be low or medium risk do not require the completion of a full BSR questionnaire
- 1.13 The process ends here as there is no further evidence required
- 1.14 If a BSR is required, or if the project/development is a critical or high-risk project the CSO and Security Architecture update the JIRA ticket with the comments as well as update the Project Respondent via mail
- 1.15 The CSO then launches a BSR assessment. The CSO logs into the OneTrust system and launches an assessment, by selecting the Assessment Automation tile, and then clicking on the 'Launch Assessment' button in the top right-hand corner of the screen. The CSO then selects the 'Vodacom Cyber Security BSR: V3' tile
- 1.16 OneTrust then sends an automated email to the Project Respondent with a link to a questionnaire that is to be completed by the Project Respondent
- 1.17 The Project Respondent completes the OneTrust assessment and submits the completed questionnaire on the OneTrust system. The Project Respondent is required to answer all relevant questions based on the solution being assessed and provide the supporting evidence requested for all relevant controls
- 1.18 An automated email is sent to the CSO from the OneTrust system, notifying them that there is an assessment that has been completed for review
- 1.19 The OneTrust BSR is reviewed for completeness and the evidence provided is sufficient
- 1.20 The CSO confirms if the BSR assessment is complete. If the BSR is not complete and/or does not have the required evidence, then the CSO reverts to the Project Respondent with feedback as to what is still required, and the process moves back to 1.17. If the BSR is complete, the process moves to 1.21 and 1.35 and 1.48

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 3 of 95



- 1.21 The CSO, having reviewed the OneTrust assessment, identifies and raises control weaknesses and associated risks that are to be addressed in OneTrust. These Risks and Controls will then be communicated to the Project Respondent via an email sent automatically from OneTrust to the Project Respondent when the risk is captured on OneTrust. This email is generated every time a Risk is raised on OneTrust
- 1.22 The Project Respondent then develops a remediation plan detailing the remedial actions and control improvements that will be undertaken to address the risks identified
- 1.23 The CSO is then required to review the Risk Remediation Plan or Control Improvement Plan to determine whether it is adequate to remove, reduce, or transfer the risks identified. The CSO will then provide feedback to the Project Respondent on whether the risks identified have been adequately remediated
- 1.24 Should the Risk Remediation Plan or Control Improvement Plan not adequately remediate the risks, then the plan is updated with a new or more in-depth Plan
- 1.25 The CSO is then required to review the updated Risk Remediation Plan. If the updated plan has adequately remediated the risks, the process continues
- 1.26 If the updated Risk Remediation Plan or Control Improvement Plan does not adequately remediate the risks, the CSO or the Secure by Design Manager may not stop the project, considering the risk levels are acceptable at 'Critical' or 'High', the process continues. The risks and prioritization are determined according to the matrix in Figure 153, which helps determine timeframes and activities that are needed to be completed
- 1.27 If the risks are not remediated, a Policy Dispensation (PD) or Security Risk Acceptance (SRA) is applied for by the Project Respondent
- 1.28 The Group Risk and Compliance (GRC) department then assesses the PD/SRA application to determine the way forward
- 1.29 If the PD/SRA is not approved, a meeting is set up by the Project Respondent to negotiate the way forward with the CSO, GRC, and Security Architecture
- 1.30 If the PD/SRA is approved, then the evidence is captured on OneTrust and the process continues
- 1.31 From 1.23, and 1.26, if the Risk Mitigation Plan is satisfactory to the CSO, or the Cyber Secure by Design Manager finds the risks acceptable for the project to continue, the process continues
- 1.32 The Approval/Go Live is then recorded on OneTrust, along with the evidence of why the decision was taken to move forward with the project
- 1.33 The JIRA ticket is then updated with notes and comments as to why the approval/go-live was granted
- 1.34 The process ends here
- 1.35 From 1.20, once the BSR is completed, the project/development is then required to have Vulnerability Scans performed
- 1.36 The types of scans that may be performed are viz. Network bases Scans, Host-based scans, Web application scans, Application scans, and Database scans
- 1.37 Once the scans are performed, the CSO must assess the risks in accordance with Vodacom's policies and control requirements and determine to determine whether the project may continue. If there are no risks to mitigate or remediate, the process continues at 1.47
- 1.38 The risks, should there be any, are then recorded on OneTrust.
- 1.39 The risks are then raised with the Project Respondent and Business for them to be able to mitigate or remediate the risks identified

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 4 of 95



- 1.40 Once the risks have been raised, the Project Respondent and Business then attempt to mitigate or remediate the risks if possible
- 1.41 If they are unsuccessful in doing so, then a PD or SRA may be applied for
- 1.42 Should the Project Respondent and Business not receive a dispensation, then a meeting is set up with various teams
- 1.43 The Project Respondent sets up a meeting with the CSO, GRC, and Security Architecture to negotiate the way forward
- 1.44 All evidence is captured onto OneTrust and the process moves to 1.31
- 1.45 Cyber Security will work with the stakeholders to determine whether projects/development requires a Penetration test as early as possible as there are cost implications that need to be considered and borne by the respective BU. If a Penetration test is not required, the evidence or considerations are captured on OneTrust, and the process moves to 1.31
- 1.46 If a Penetration Test is required, the CSO informs the Project Respondent and Business that a Penetration Test is required and that budget is required for the testing.
- 1.47 Business is required to provide the budget for the Penetration Test. Should the budget not be approved, the process moves to point 57
- 1.48 However, if the budget is approved, the Project Respondent engages the Internal Vodacom Penetration Test department and scopes the Penetration Test together with the Penetration Test Team and the CSO
- 1.49 The Vodacom internal Penetration Test department engages the vendor to perform a Penetration Test
- 1.50 The Penetration Test helps identify risks in the project/development. If there are no risks identified after the Penetration Test is run, then the evidence is captured on OneTrust and the process moves to 1.31
- 1.51 Should some risks are identified after the Penetration Test, the risks are recorded on OneTrust or Jira depending on the type of SPDA being run at the time.
- 1.52 The risks are also raised with the Project Respondent and Business
- 1.53 The risks that were raised by the CSO are then remediated by the Project Respondent
- 1.54 Should the Project Respondent be successful in remediating the risks a further Validation Penetration Test is carried out to determine if the risks have been remediated and evidence provided. Should the Validation Penetration Test be successful, then the process reverts to 1.50
- 1.55 However, if the risks raised in 1.52 are not remediated, then the Project Respondent applies for a Dispensation. If a dispensation is granted, then the information is recorded on OneTrust and the process moves to 1.31
- 1.56 If the dispensation was not granted in 1.55, the project can still move forward at the discretion of the CSO, Cyber Security Manager, and Business, provided there are no critical and high risks present
- 1.57 From 1.31, if the approval is not granted, the CSO and the Project Respondent need to reach an agreement as to how the project will move forward. The process then moves to 1.33

The complete process is attached below:

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 5 of 95



SPDA Process.vsdx



SPDA Process.pdf

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 6 of 95



2. JIRA: Viewing, Moving Tickets along the process, and Closing Tickets in JIRA

Once a ticket is created in JIRA as part of a ‘Feature’ or as part of completing the Initial Questionnaire in Confluence, the CSO can view the tickets via the Cyber Security JIRA Kanban board. The CSO will also receive an email informing them that they have a new ticket assigned to them. The assigning of the tickets is done automatically by the JIRA system

Figure 2

The board can be filtered by CSO, which will then display all tickets assigned to the CSO

Figure 3

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 7 of 95

The CSO then double-clicks on the relevant ticket to open the ticket

The screenshot shows the Jira interface for a project named 'SPDA Cyber Security'. A ticket titled 'SPDACS-2736' is open. The ticket details pane is visible, showing the 'SPDA Backlog' section. The 'Development' field is highlighted with a yellow box. The ticket has been moved to the 'Backlog' stage.

Figure 4

The CSO can then select the 'Backlog' and move the ticket through the various stages of the SPDA process

The screenshot shows the Jira interface for a project named 'SPDA Cyber Security'. A ticket titled 'SPDACS-2789' is open. The ticket details pane is visible, showing the 'SPDA Backlog' section. The 'Development' field is highlighted with a yellow box. The ticket has been moved to the 'Backlog' stage.

Figure 5

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 8 of 95



After the CSO started to attend to the ticket in JIRA, they will move the ticket into the Initial Assessment phase on the JIRA Kanban board by either selecting from the dropdown and dragging the ticket to the Initial Assessment Column on the JIRA board,

This screenshot shows a JIRA issue page for ticket SPDACS-2789. The ticket is titled "This is an SPDA CyberSecurity task for: Demo for PI committed SPDA's". The workflow transition "BL-> Initial Assessment > INITIAL ASSESSMENT" is highlighted with a yellow box. The ticket details include reporter Kesh Munillal, development status (Create branch, Create commit), and various labels like None, Impact Area, Business Projects, Target Date: Analysis, Date Required, Parent Link, Priority (Medium), Automation (Rule executions), Zendesk Support, and Tempo (Open Tempo). The ticket history shows comments from Kesh Munillal, Celeste Viviers, and Shaida D'avico. The right sidebar shows recent activity and a search bar.

Figure 6

or by selecting the relevant ticket and dragging and dropping the ticket from 'Backlog' into the 'CSO in Progress' column of the Cyber Security JIRA Kanban board

This screenshot shows the JIRA Kanban board for the SPDA Cyber Security project. The board has several columns: BACKLOG, CSO IN PROGRESS, BU STAGED, BSR SENT, BSR REVIEW, RISK MITIGATION & RE..., and DONE. A yellow box highlights the "CSO IN PROGRESS" column. Tickets in this column include "DCB: API Configuration on Nokia HLD" (Carol-Ann), "SMME Portal HLD" (Laru Pillay), "BRS and HLD for FS1-2008" (Franck Vodacom), "Architecture Approval for Nokia AMS" (Carl Heinz Uys), "Architecture approval" (Carl Heinz Uys), "Vodafone Life Assurance: Third Party - Quintica" (Jabulani Sigasa), "Self-Service Merchant Onboarding - VFS Digital + VFS Payments Services" (Mpumelelo Ndaba), and others. The right sidebar shows a summary of completed tasks (DONE 153) and a search bar.

Figure 7

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Figure 8

From here, the CSO can move the ticket through the various stages of the process by either selecting from the dropdown

Figure 9

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 10 of 95



or by dragging and dropping the ticket into the relevant column on the Cyber Security JIRA Kanban board

The screenshot shows a JIRA Kanban board for the 'SPDA Cyber Security' project. The board has six columns: BACKLOG, CSO IN PROGRESS, BU STAGED, BSR REVIEW, RISK MITIGATION, and DONE. A ticket titled 'K - Test' is selected in the CSO IN PROGRESS column. The ticket details show it's assigned to Kesh Munillal and has the ID SPDACS-2736. The ticket description states: 'This SPDA CyberSecurity task is for demo purposes only - Demo for SPDA Process'.

Figure 10

Once the CSO has ascertained the information required to log a OneTrust Assessment, they will log into OneTrust and launch the assessment if required. If there is no OneTrust assessment to be completed, or the OneTrust assessment has been completed and the decision has been made concerning the way forward, the CSO will capture the evidence and select 'Done', or drag the ticket to the 'Done' column of the Cyber Security JIRA Kanban board and complete the information required to close the ticket and select the 'SPDA IA --> Done'

The screenshot shows the JIRA ticket detail view for SPDACS-2736. The ticket is titled 'K - Test'. A modal window titled 'SPDA IA --> Done' is open, showing fields for Actual Completion Date (set to June 29, 2022), Resolution (Please select...), and Comment. The comment field contains the text: 'The ticket will be automatically closed when the OneTrust assessment is completed.'

Figure 11

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe
Title: SPDA How to Guideline
Page 11 of 95



3. Initial Qualifying Questionnaire

As there are one of two processes that are followed to request the SPDA assessments, i.e. the PI initiatives Process, and the non-PI initiatives Process, we have different Initial Qualifying Questionnaires that are completed due to the amount of information already known regarding the initiatives

3.1 PI Process Initial Qualifying Questionnaire:

Details [Cyber-Security](#) Privacy (Popi) Business Risk test link

New Application?

Will there be any new interface/integration/system involved? (Migrated on 15 Apr 2022 10:34 UTC)

Project Development Type?

Is this project developed in-house or procured partially/fully external? (Migrated on 15 Apr 2022 10:34 UTC)

Customer Facing?

Will there be a customer-facing interface? (Migrated on 15 Apr 2022 10:34 UTC)

Sensitive Data?

Will there be any customer data/sensitive business data processed? (Migrated on 15 Apr 2022 10:34 UTC)

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 12 of 95



Impact on Data Security Standards/Regulations?

Is there an impact of demand/project regarding SOx (Public Company Accounting Reform and Investor Protection Act), PCI-DSS (Payment Card Industry Data Security Standard), GDPR/POPI (Private Data Law)? (Migrated on 15 Apr 2022 10:34 UTC)

CyberSecurity Prioritisation

Low

- No new systems or interfaces introduced
- Only minor system configurations
- Existing approved supplier using existing remote access methods
- Low ZA impact changes already assessed by Group Cyber Security.
- No SOx, PCI DSS impacts.
- Low impact changes to 3rd party provided services that have already been assessed by Supplier Security (Cyber GRC).

Med

- New internal interfaces introduced
- Single new internal system introduced.
- Existing approved supplier changing to a new approved remote access method.

-
- No SOx, PCI DSS impacts.

- Employee data but no Customer data.

- Infrastructure projects

High

- New external interfaces introduced
- New internet facing system introduced.
- Multiple new internal systems introduced.
- New supplier using an approved remote access method.
- SOx impacts.
- Involves Customer data and/or sensitive business data
- Regulatory
- Time to Gate2<1 month
- PI\PCI Information

Critical

- New hosting environment and/or network introduced. (Public Cloud?)
- New remote access solution and/or non-standard remote access requirements.
- SOX/ PCI DSS impacts
- Customer facing system.
- Involves C4 data.
- Regulatory
- Internet facing Systems
- Customer mobile apps (Migrated on 15 Apr 2022 10:34 UTC)

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 13 of 95



Details Cyber-Security **Privacy (Popi)** Business Risk test link

Categories of Customer Personal Data

Please indicate whether any of the following categories of customer personal data are to be processed (Multiple selections allowed)
(Migrated on 15 Apr 2022 10:34 UTC)

Categories of Employee Related Personal Data

Please indicate whether any of the following categories of Employee Related personal data are to be processed (Multiple selections allowed)
(Migrated on 15 Apr 2022 10:34 UTC)

Categories of "Visitor" Related Personal Data

Please Indicate whether any of the following categories of "visitor" related personal data are to be processed (Multiple selections allowed)
(Migrated on 15 Apr 2022 10:34 UTC)

Categories of Supplier Related Personal Data

Details Cyber-Security Privacy (Popi) **Business Risk** test link

Product or Service type?

The purpose of this field is to determine whether the initiative you're creating/working on is either a product or a service – is it new or existing (e.g. data bundles)? is it an enhancement, innovation, competition, promotion or technology initiative (e.g. system Upgrades, patches, new technology or feature, etc.) or something that does not fall in any of the categories listed. (Migrated on 15 Apr 2022 10:34 UTC)

Product or Service Description

(Migrated on 15 Apr 2022 10:34 UTC)

Target market?

The purpose of this field is to establish who the customer is and which business unit is impacted. (Migrated on 15 Apr 2022 10:34 UTC)

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 14 of 95



Target Market Description

(Migrated on 15 Apr 2022 10:34 UTC)

Regulatory requirement?

▼

The purpose of this field is to determine if the initiative has a regulatory impact. (Migrated on 15 Apr 2022 10:34 UTC)

Regulatory Requirement Description

(Migrated on 15 Apr 2022 10:34 UTC)

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe

Page 15 of 95



3.2 Non-PI initiatives Initial Qualifying Questionnaire

Initiative Information:					
Initiative JIRA Reference: This is an example : Jira CROAD-1311					
Initiative Info Required				Initiative Owner Response	
Planned Go Live Date					
Project being initiated because of an Audit/Risk/Security remediation finding ?					
Is there a regulatory impact (e.g. lodgment, license required)					
What is the percentage of customers impacted					
Does this application reference a known and agreed architecture pattern?					
If yes to above, please provide reference to the initial approval					
Initiative Stakeholders:					
Stakeholder Type				Stakeholder Name	
Application Owner					
Project Manager					
Technical Lead					
Initiative Documentation Reference/s:					
Documents (Please insert all relevant Initiative documents here. These are examples)				Document / Confluence Link	
Feature Statement					
Memo					
HLD					
LLD					
Please note that it is required that this questionnaire is completed and submitted with the JIRA tickets that are created on the SPDA team JIRA board/s.					
Assurance Area / Team	JIRA project/ Key Ref:	Issue Key	SPOC "Assignee"	JIRA Reference for this submission:	
Business Risk	SPDA Business Risk	SPDABR	Prince Shonhiwa	Insert ref here	
Privacy (POPI)	SPDA Privacy (POPI)	SPDAP	Matome Bopape	Insert ref here	
Cyber Security	SPDA Cyber Security	SPDACS	Insert Relevant Person	Insert ref here	
GRC (Governance, Risk & Compliance)	SPDA GRC	CGVZA	Walter Piepmeyer	Insert ref here	
Principle:					
Each Initiative will require submission of this questionnaire to SPDA					
It is the responsibility of the Initiative owner to drive SPDA within their delivery cycle					
Complete every single field below					
Product / Service Description & Scope:					
Description & Key Dependencies:					
Contained in an existing document? (If ticked, please attach the memo/business spec/low level design document to the table: Initiative Document References)				<input type="checkbox"/>	
Not Contained in an existing document				<input type="checkbox"/>	
Please populate a high level description of the products / services and a list of key dependencies here:					
Is there a change to an existing project or process? Please tick all of the following that apply.(Where we have previously conducted a review, we will need to record what is about to change, AND whether or not a new compliance review is required. We may ask you to refer to internal records to understand what was the original approval)					
Mandatory Questions					Additional Notes/Clarification
This is a new feature / service / product	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Are you using existing infrastructure to implement?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Do you need a new environment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Is this a new commercial offering to customers?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Is this an enhancement/addition to an existing commercial offering to customers?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Product / service stays exactly the same - simply introducing a new supplier	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Business / Partnering model for this product / service					Additional Notes / Clarification
Is this a new business model	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
VC Only product / service	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Partner ONLY : (VC Branded)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Partner ONLY : (NOT VC Branded)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Combined VC and Partner initiative (VC Branded)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	
Combined VC and Partner initiative (NOT VC Branded)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Partial	<input type="checkbox"/> N/A	

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT



Please tick all of the following Technical detail that applies:					
Design Question	Question Definition	Answer			Additional Notes/Clarification
Microservice/API/Webservice Initiative		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
Product is customer facing?		Enterprise <input type="checkbox"/>	Consumer <input type="checkbox"/>	VC Internal <input type="checkbox"/>	N/A <input type="checkbox"/>
Product includes a mobile application		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
Product is Internet facing		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
product supports		Voice Calls <input type="checkbox"/>	Video/Data <input type="checkbox"/>	SMS/Text <input type="checkbox"/>	N/A <input type="checkbox"/>
product solution contains a Vodacom SIM		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
Is a cloud based service		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
product/service will process purchases		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
product/service will process payments		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
There will be development or code changes to the application		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
There will be configuration changes to the application		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
The architecture of the solution changes		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
Any existing Audit, risks, or vulnerabilities that affect the system, services, or business process		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
Any existing Audit, risks, or vulnerabilities that affect the application directly or indirectly		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/> Please elaborate
When was the last Penetration Test done on the product?		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>

Technical Hosting Information:					
Which of the following is your application hosted on?	Cloud <input type="checkbox"/>	On Prem <input type="checkbox"/>	Third Party <input type="checkbox"/>		
If Third Party is ticked, please provide:					
Third Party Information Required	Answer:			Please Elaborate	
When was the last third party assessment done	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	Provide date
Any existing Audit, risks, or vulnerabilities that affect the application directly or indirectly	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	Attach the risk register
Is the third party assessment still valid?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	Attach the evidence here
Is there a new partner / vendor / supplier involved with this product / service?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Other Comments					

Privacy Specific Information:					
Click on this link to get guidance on what is considered as personal information.					
Type of Personal Data					Please Elaborate
Customer Personal Data					
Account Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Authentication Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Financial Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Customer Care Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Content Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Call, Internet and/or Television Traffic Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Location Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Data about Device	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Data from Device	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Profiling Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Public Identity Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Special categories of Personal Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Biometric identifiers or similar physical-based data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Other:					
Employee Data Types					
Recruitment Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Sensitive Employee Personal Data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Employment Details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Salary and Payment Details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Performance Details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
HR Administration and Support	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Employee Authentication or Log in Details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Employee Wellbeing details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Health and Safety Records	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Biometric and similar physical based details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Content of Employee Communications	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Device Based or related data for corporate devices	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Monitoring of Employees	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Other:					
Supplier Related Personal Data:					
Supplier's Employee data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Contract details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Electronic Signature	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Biometric Signature	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Monitoring of Supplier's Employees	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Other:					
Visitor Related Personal Data					
Visitor details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Biometric identifiers and similar physical-based data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Partial <input type="checkbox"/>	N/A <input type="checkbox"/>	
Other					



Initial Qualifying
Questionnaire.xlsx

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 17 of 95



4. OneTrust: Launch SPDA Assessment BSR

Login Screen:

The screenshot shows the OneTrust login interface on the left and the platform's main dashboard on the right. The login screen has fields for 'Email Address' (Kesh.Munillal@vcontractor.co.za) and a 'Next' button. The dashboard features the OneTrust logo and the tagline 'The Trust Intelligence Platform: Visibility, Action & Automation Across Trust Domains'. It highlights four main domains: Privacy & Data Governance, GRC & Security Assurance, Ethics & Compliance, and ESG & Sustainability, each with its own set of sub-modules. At the bottom, there are sections for 'Automated Intelligence' and 'Stakeholder Engagement'.

Figure 12

You will be able to view the assessments that have been sent out to the Business, and you are also able to launch an assessment from here

The screenshot shows the Vodafone Privacy Portal's 'Assessments' page. The left sidebar includes options like 'ASSESSMENT AUTOMATION', 'Dashboard', 'Assessments' (which is selected), 'Active', 'Archive', 'Recycle Bin', 'Risk Register', 'Reports', 'setup', and 'Templates'. The main area displays a table of assessments with columns: ID, Name, Stage, Result, Residual Risk Level, Residual Risk Score, Organization, Respondent, Approver, and a status bar. The table lists various tests and their details, such as 'K-Test S7' (Not Started), 'Test K56' (Not Started), 'Test - PA Overwrite Test - PPPP' (In Progress), etc. At the bottom, it shows 'Showing 1 - 20 of 237'.

Figure 13

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 18 of 95



To launch an assessment, the CSO will select the 'Launch Assessment' button

The screenshot shows the OneTrust Privacy, Security & Governance interface for Vodafone. The left sidebar has sections like ASSESSMENT AUTOMATION, Dashboard, Assessments (Active, Archive, Recycle Bin), Risk Register, Reports, Setup, and Templates. The main area is titled 'Assessments' and shows a table of current assessments. A yellow box highlights the 'Launch Assessment' button at the top right of the table header.

Figure 14

The Launch assessment screen will be displayed. Select the Vodacom Cyber Security BSR V3

The screenshot shows the 'Launch Assessment' screen within the Vodafone Privacy Portal. It displays a grid of various assessment templates. A yellow arrow points to the 'Vodacom Cyber Security BSR V3' template, which is highlighted with a yellow box. This template card includes a green wrench icon and a 'Select' button.

Figure 15

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 19 of 95



The CSO will complete the editable boxes, i.e., 'Name', 'Approver', and 'Respondent'. The 'Organisation' field will already contain 'Vodacom South Africa'. If it is a different organization, this field needs to be changed. Then select the 'Launch' button (bottom right of screen). This will enable One-trust to send an email with a link to the OneTrust assessment to the Project Respondent for completion

The Approver in most of the instances will be the CSO responsible for reviewing the project but can also be assigned to a different person for approval. Respondents can be multiple respondents depending on the project. To add respondents, simply select their name from the dropdown

The screenshot shows the 'Enter Assessment Details' page of the OneTrust platform. On the left, there's a sidebar with navigation links like 'Assessment Automation', 'Dashboard', 'Assessments' (Active, Archive, Recycle Bin), 'Risk Register', 'Reports', 'Setup', and 'Templates'. The main area has a title 'Enter Assessment Details' and four input fields with validation stars: 'Name' (with placeholder 'Enter Assessment Name'), 'Organization' (set to 'Vodacom South Africa'), 'Respondent' (placeholder 'Select Respondent(s)'), and 'Approver' (placeholder 'Select Approver(s)'). Below these fields are two checkboxes: 'Assign sections while launching this assessment' and 'Assign approver workflow stages while launching this assessment'. At the bottom right, there's a 'Launch' button.

Figure 16

The Project Respondent then receives a mail requesting them to complete the OneTrust Assessment

Once the Project Respondent has completed the assessment, the CSO will receive an email from OneTrust informing them that an assessment is ready for review

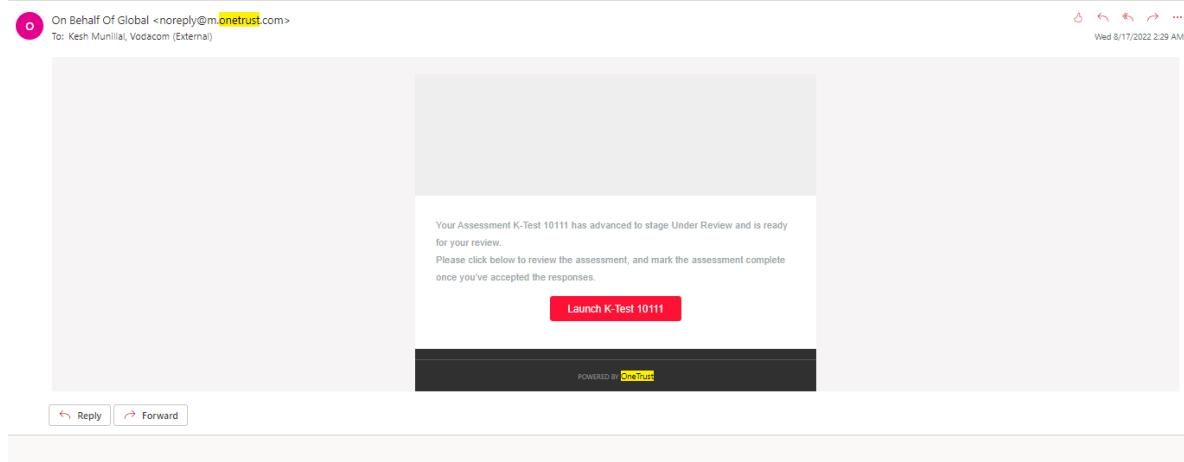


Figure 17

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT



The CSO then selects the 'Launch' assessment button in the body of the mail

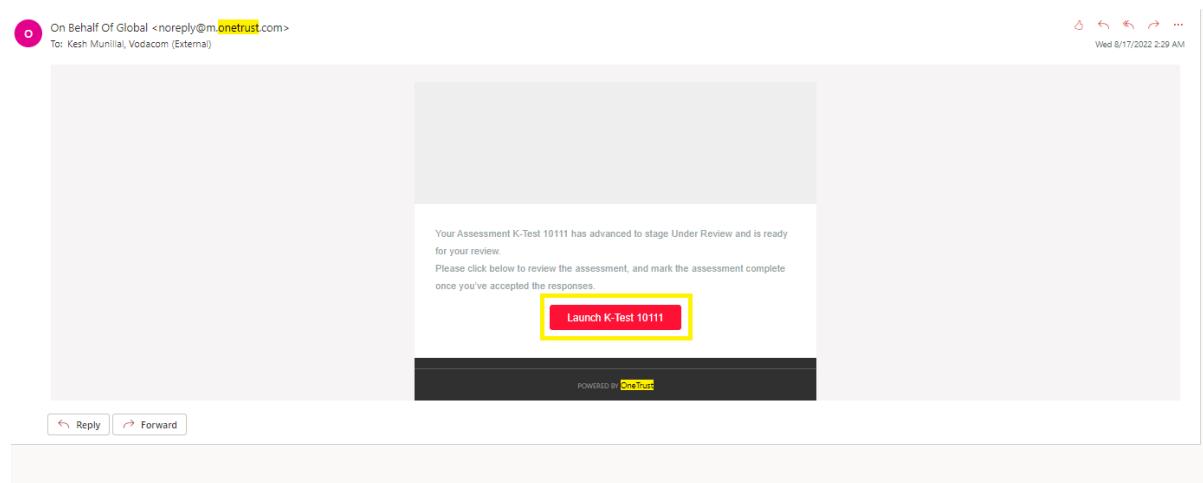


Figure 18

Once the CSO has completed reviewing the assessment, they click on the 'Finish Review' button

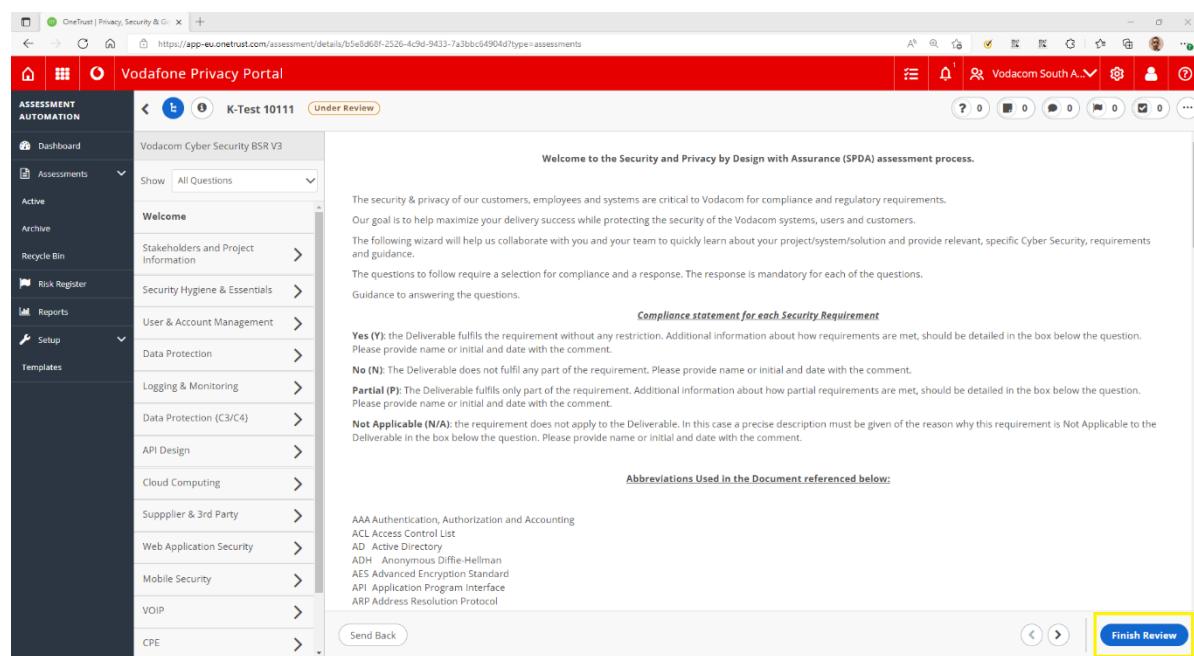


Figure 19

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 21 of 95



The CSO must either ‘Approve’ or ‘Decline’ the Ticket in the ‘Results’ field, complete the ‘Comments’ field and press the ‘Confirm’ button to proceed

The screenshot shows the 'Complete Assessment' dialog box overlaid on the Vodafone Privacy Portal. The dialog box contains instructions and three dropdown menus for selecting the result of the assessment. The 'Result' dropdown is highlighted with a yellow box. Below it is a 'Comments' text area, also highlighted with a yellow box. At the bottom right of the dialog box is a 'Confirm' button, which is also highlighted with a yellow box.

Figure 20

The stage will then move to ‘Completed’, which indicates that the SPDA has been completed successfully

ID	Name	Stage	Result	Residual Risk Level	Residual Risk Score	Organization	Respondent	Approver
34221	K-Test 10111	Completed	Approved	----	----	Vodacom South Africa	Kesh Munnilal	Kesh Munnilal
34146	K-Test 57	Not Started	----	----	----	Vodacom South Africa	Kesh Munnilal	Kesh Munnilal
34122	Test K56	Not Started	----	----	----	Vodacom South Africa	Kesh Munnilal	Kesh Munnilal
33910	Test - PA Overwrite Test - PPPP	In Progress	----	----	----	Vodacom South Africa	Michael Machinlike	Michael Machinlike
33909	Test - PA Overwrite Test - GGGG	Completed	Approved	💬	72	Vodacom South Africa	Michael Machinlike	Michael Machinlike
33745	Test - PA Overwrite Test - copied t...	Completed	Approved	💬	52	Vodacom South Africa	Michael Machinlike	Michael Machinlike
33744	Test - PA Overwrite Test	Completed	Approved	💬	67	Vodacom South Africa	Michael Machinlike	Michael Machinlike
33574	Test Product Test	In Progress	----	----	----	Vodacom South Africa	Michael Machinlike	Michael Machinlike
33544	Product and Services: Testing	Not Started	----	----	----	Vodacom South Africa	Masiza Outu	Mamo Madur
33424	SPDA for Implementation of DNS ...	Under Review	----	----	----	Vodacom South Africa	Zanele.Mkhomazi@vodacom.co.za, p...	Pakama Matro
33414	test BSR	In Progress	----	----	----	iOTrix Pty Ltd	Constantine Nyamandi	Renico Koen
33299	Network Testing	Completed	Approved	----	----	Vodacom South Africa	Masiza Outu	Mamo Madur
33174	Test for legitimate interest	Under Review	----	----	15	Vodacom South Africa	Sherly Mphahlele	Matome Bopa
33128	B2B Transformation SPDA Cyber T...	In Progress	----	----	----	Vodacom South Africa	Marietjie Lancaster, luciano.boretto@...	Lucy Motsieloa, Reuel M...
33057	ABC Test	Not Started	----	----	----	Nexio	Zinta Strydom	Zinta Strydom

Figure 21

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT



The CSO then logs into JIRA and accesses the relevant Ticket. The CSO then moves the ticket to the 'SPDA IA --> Done', completes the relevant information, and selects the 'SPDA IA --> Done' in blue at the bottom of the screen

The screenshot shows a JIRA ticket editing interface. The ticket is titled "SPDA IA --> Done". The main body of the ticket contains several input fields:

- "Actual Completion Date": A date input field.
- "Resolution": A dropdown menu set to "Please select...".
- "Parent Link": A dropdown menu set to "Choose a parent to assign this issue to".
- A large "Comment" area with rich text editing tools (bold, italic, underline, etc.).

A yellow box highlights the entire form. At the bottom right of the dialog is a blue button labeled "SPDA IA --> Done".

Figure 22

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 23 of 95



5. OneTrust: Cyber Security Assessment – Baseline Security Requirement

Welcome

The screenshot shows the OneTrust interface for the Vodafone Privacy Portal. The left sidebar lists various sections like Dashboard, Assessments, Reports, and Setup. The main area displays a list of questions under the 'Welcome' section, each with a red button containing a number indicating the count of deliverables. The first question is 'Stakeholders and Project Information' with 10 deliverables. Other visible questions include 'Security Hygiene & Essentials' (26), 'User & Account Management' (31), 'Data Protection' (4), 'Logging & Monitoring' (4), 'Data Protection (C3/C4)' (1), 'API Design' (1), 'Cloud Computing' (1), 'Supplier & 3rd Party' (1), 'Web Application Security' (1), and 'Mobile Security' (1). The right side contains a welcome message, project details, compliance statements, abbreviations, and a 'Submit' button.

Figure 23

5.1 Select Stakeholder and Project Info

Questions 1.1 to 1.10

The screenshot shows the 'Stakeholders and Project Information' section of the assessment. It lists seven questions numbered 1.1 through 1.7. Question 1.1 asks for the project name, question 1.2 for Jira initiative/project reference, question 1.3 for project type, question 1.4 for Go-Live date, question 1.5 for business unit, question 1.6 for business owner details, and question 1.7 for project lead. Each question has a text input field with a rich text editor toolbar below it. The right side of the screen includes a 'Submit' button.

Figure 24

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 24 of 95



OneTrust | Privacy, Security & GRC

Vodafone Privacy Portal

k-Test 10112 Not Started 0/90 0%

ASSESSMENT AUTOMATION

Assessments

- Active
- Archive
- Recycle Bin

Risk Register

Reports

Setup

Templates

Vodafone Cyber Security BSR V3

Show All Questions

Welcome

Stakeholders and Project Information * 10

1.3 *Please indicate the type of project.

New Service / Solution / Product
Enhancement to existing Service/Product
Proof Of Concept
Other

Explain your answer below.
Enter Reason for response here.

1.4 *Project Go-Live Date

Choose a Date

1.5 *Please indicate the Business Unit the project is initiated from

Type or select an option

1.6 *Please provide the Business Owner details for the project

Enter your answer here.

Submit

Figure 25

OneTrust | Privacy, Security & GRC

Vodafone Privacy Portal

k-Test 10112 Not Started 0/90 0%

ASSESSMENT AUTOMATION

Assessments

- Active
- Archive
- Recycle Bin

Risk Register

Reports

Setup

Templates

Vodafone Cyber Security BSR V3

Show All Questions

Welcome

Stakeholders and Project Information * 10

1.5 *Please indicate the Business Unit the project is initiated from

Type or select an option

1.6 *Please provide the Business Owner details for the project

Enter your answer here.

Submit

Figure 26

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe
Page 25 of 95

Title: SPDA How to Guideline

The screenshot shows a web-based assessment portal for Vodafone. The left sidebar has a dark theme with navigation options like Dashboard, Assessments, Active, Archive, Risk Register, Reports, Setup, and Templates. The main area is titled 'Vodafone Privacy Portal' and shows an assessment named 'k-Test 10112' which is 'Not Started'. The progress bar indicates 0/90 questions completed at 0%. The current section is 'Stakeholders and Project Information' with 10 questions. Questions 1.7 and 1.8 are displayed:

- 1.7** *Please provide the Project Lead associated with the project.
- 1.8** *Please Provide the Architect associated with the project.

Both questions have a rich text editor with standard toolbar icons (Bold, Italic, Underline, etc.) and a placeholder 'Enter your answer here.' Below each question are three small circular buttons.

Figure 27

This screenshot shows the continuation of the assessment. The sidebar and overall layout remain the same. The current section is 'Stakeholders and Project Information' with 10 questions. Questions 1.9 and 1.10 are displayed:

- 1.9** *Please indicate the Suppliers/Vendors involved in the project.
- 1.10** *Please indicate what is the solution designed to deliver to the customer? Please provide an overview of the proposed product/solution.

Both questions have a rich text editor with standard toolbar icons and a placeholder 'Enter your answer here.' Below each question are three small circular buttons.

Figure 28

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 26 of 95



5.2 Security Hygiene and Essentials

Questions 2.1 to 2.35

2.1 Platform Design and Build

Platform design must be compliant with the existing Vodafone Security Standards, Guidance and Requirements.

- Tier 3 Standard: System and Service Security Zoning
- Security Zoning Definition Document
- Tier 3 Standard: Remote Access
- Tier 3 Standard: Cryptography
- Information Security Classification and Protection DR
- Secure System Development Lifecycle Detailed Requirements
- DNS Security Definition Document
- Cloud Computing Security Detailed Requirements
- Access and Authentication Detailed Requirements

Reference:

- CSB Control In Scope - Control 13.1.3

Note - Other policies may be applicable based on the scope of product/service.

[View Supporting Attachments \(9\)](#)

Type or select an option

*** Explain your answer below.**

Enter Reason for response here.

Submit

Figure 29

2.2 Platform Design and Build

Production systems shall not use the same environment as stage, testing, development or pre-production systems.
Each environment must have a dedicated purpose.

Type or select an option

*** Explain your answer below.**

Enter Reason for response here.

2.3 Network Segregation

All traffic between systems shall be compliant with the Vodafone Network Security Detailed Guidance and meet the Vodafone Network Security Detailed Requirements.

Submit

Figure 30

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 27 of 95

The screenshot shows a web-based assessment tool. On the left, a sidebar lists various sections like Dashboard, Assessments, Active, Archive, Recycle Bin, Risk Register, Reports, Setup, and Templates. The main area is titled 'Vodafone Privacy Portal' and shows an assessment named 'Vodafone Cyber Security BSR V3'. A progress bar indicates 'Not Started' with 0/90 questions completed at 0%. The current section is 'Security Hygiene & Essentials' with 28 questions. Question 2.3 is displayed, asking about 'Network Segregation'. It states: 'All traffic between systems shall be compliant with the Vodafone Network Security Detailed Guidance and meet the Vodafone Network Security Detailed Requirements.' Below this is a 'Reference Documents Below' section listing various security documents. There is also a 'Reference:' section with a link to 'CSB Control in Scope - Control 13.1.3'. A text input field with placeholder 'Type or select an option' and a rich text editor are present. The question ends with a 'Submit' button.

Figure 31

This screenshot continues from Figure 31. It shows the next question in the assessment, which is also about 'Network Segregation'. The question states: 'All data traffic coming from the Internet or other untrusted networks shall terminate in a reverse proxy which may validate and pass the request on to application servers. This reverse proxy physically separates trusted and untrusted interfaces.' Below this is a 'References:' section with links to 'Vodafone Network Security Detailed Requirements' and 'Tier 3 Standard: System and Service Security Zoning'. A 'Secure System Development Lifecycle Detailed Requirements' link is also listed. The interface includes a 'Type or select an option' input field and a rich text editor. The question ends with a 'Submit' button.

Figure 32

Figure 33

Figure 35

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 29 of 95

The screenshot shows a web-based assessment tool. The left sidebar has a dark theme with white text, listing 'ASSESSMENT AUTOMATION' and several menu items: Dashboard, Assessments (Active, Archive, Recycle Bin), Risk Register, Reports, Setup, and Templates. Under 'Assessments', there's a dropdown for 'Vodafone Cyber Security BSR V3' which is currently selected. A sub-menu for 'Security Hygiene & Essentials' is open, showing numbered questions from 2.1 to 2.11. Question 2.7 is highlighted with a red circle containing the number '2.7'. The main content area shows two questions related to 'Network Services'. Question 2.7 asks: 'Firewall rules and similar traffic filters shall not include the 'ANY' value for SOURCE or DESTINATION, instead either a host or subnet shall be given.' It includes a 'References:' section pointing to 'CSB Control 13.1.1-C' and a rich-text editor for 'Explain your answer below.' Question 2.8 follows, with a note: 'Firewall rules and similar traffic filters shall not include the 'ANY' value for ports. A valid port number or port range shall be given for all required rules.' Both questions have a 'Type or select an option' input field and a 'Submit' button at the bottom right.

Figure 36

This screenshot continues the assessment from Figure 36. The left sidebar remains the same. The main content area now shows Question 2.8, which asks: 'Firewall rules and similar traffic filters shall not include the 'ANY' value for ports. A valid port number or port range shall be given for all required rules.' Below it is Question 2.9, which asks: 'Bidirectional traffic shall be detailed in separate firewall access rules (i.e. one rule for each traffic flow direction).' Both questions have their respective 'Type or select an option' input fields and a 'Submit' button at the bottom right.

Figure 37

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 30 of 95

The screenshot shows a web-based assessment tool. The left sidebar has sections for Dashboard, Assessments (Active, Archive, Recycle Bin), Reports, Setup, and Templates. Under Assessments, 'Vodafone Privacy Portal' is selected. The main area shows an assessment titled 'k-Test 10112' which is 'Not Started'. There are 0/90 questions completed at 0%. A red banner at the top says 'Vodafone Privacy Portal'. The current question is 2.9, titled 'Network Services', with a note: 'Bidirectional traffic shall be detailed in separate firewall access rules (i.e. one rule for each traffic flow direction)'. Below this is a text input field with a rich text editor toolbar and a placeholder 'Enter Reason for response here.' At the bottom right of the question area are back, forward, and submit buttons.

Figure 38

This screenshot is identical to Figure 38, showing the same assessment task for 'Network Services'. The question number has changed to 2.10, and the note has been updated to: 'Access services (e.g. SSH, HTTPS, RPC) shall be exclusively bound to the interface/port they are going to be serving. If they need to be reused, it has to be documented in the design.' The rest of the interface, including the sidebar, question details, and footer buttons, remains the same.

Figure 39

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 31 of 95

OneTrust | Privacy, Security & Compliance

Vodafone Privacy Portal

k-Test 10112 Not Started 0/90 0%

ASSESSMENT AUTOMATION

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

Vodafone Cyber Security BSR V3

Show All Questions

Security Hygiene & Essentials 26

2.11 * Does the current product/service review require the implementation of New Network Elements (ie, Routers / Switches / Firewalls/ WLAN devices)?

Yes No

* Explain your answer below.

Enter Reason for response here.

2.21 * Traffic Monitoring

Security devices (e.g. intrusion detection or intrusion prevention systems or Web application firewalls) shall be deployed to monitor traffic between networks based on the Systems and Services Security Zoning model.

References:

- CSB Control 13.1.1-A

Type or select an option

Submit

Figure 40

OneTrust | Privacy, Security & Compliance

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

ASSESSMENT AUTOMATION

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

Vodafone Cyber Security BSR V3

Show All Questions

2.21 * Traffic Monitoring

Security devices (e.g. intrusion detection or intrusion prevention systems or Web application firewalls) shall be deployed to monitor traffic between networks based on the Systems and Services Security Zoning model.

References:

- CSB Control 13.1.1-A

Type or select an option

* Explain your answer below.

Enter Reason for response here.

2.22 * Documentation

Save and Exit Submit

Figure 41

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 32 of 95

Figure 42

Figure 43

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 33 of 95

The screenshot shows a web-based assessment tool for Vodafone. The left sidebar lists various sections like Dashboard, Assessments, Active, Archive, Risk Register, Reports, Setup, and Templates. Under Assessments, 'Vodafone Cyber Security BSR V3' is selected. A sub-menu for 'Assessments' shows 'Show All Questions' and a list of questions under '2.24 Documentation'. The questions include:

- 2.27 Hardening Features
- 2.28 Hardening Features
- 2.29 Patch Management
- 2.30 Patch Management
- 2.31 Anti-Malware
- 2.32 Security Testing
- 2.33 Security Testing
- 2.34 Backup & Restore
- 2.35 Backup & Restore

Below these are sections for User & Account Management (31), Data Protection (4), Logging & Monitoring (9), and Data Protection (C3/C4) (1). The main content area for '2.24 Documentation' asks for documentation about user profiling and management, with a reference to CSB Control 9.2.1. It includes a text input field for explaining the answer and a rich text editor.

Figure 44

This screenshot shows the same assessment interface as Figure 44, but with different questions highlighted. The '2.25 Documentation' section is still present, asking for updated documentation if a system is modified. The '2.26 Hardening Features' section is now highlighted, stating that individual components of the system (such as web servers, operating systems, databases, API protocols, interfaces, network equipment) shall be hardened according to security best practices. It also mentions that software packages, applications, and services not required shall be deactivated or removed. The right side of the screen includes standard browser controls and a toolbar with icons for search, refresh, and other functions.

Figure 45

Vodafone Privacy Portal

ASSESSMENT AUTOMATION

k-Test 10112 In Progress 0/90 0%

2.26 Hardening Features

The individual components of the system (such as web server, operating system, database, API protocols, interfaces, network equipment) shall be hardened according to security best practices.

Software packages, applications and services that are not required shall be deactivated or removed from the system.

If in doubt, please refer to the Group Cybersecurity Policy Library at <https://vodafone.sharepoint.com/sites/groupsecurity/policies> for the hardening guidelines.

In case of partial compliance, state the non-compliant point(s) from the above.

References:

- Vodafone Hardening Guides
- Cyber Security Testing DR
- Infrastructure Security Hardening Definition
- Generic Network Node Hardening Guideline v1
- T3 High Level Standard for TLS Hardening v1.0
- High Level Standard Mobile Device Management v1.0
- CSB Control 13.1.1-H
- CSB Control 13.1.1-R
- CSB Control 18.2.3-C

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit | Submit

Figure 46

Vodafone Privacy Portal

ASSESSMENT AUTOMATION

k-Test 10112 In Progress 0/90 0%

2.27 Hardening Features

A description of the hardening settings shall be provided in detail. The Security team shall be engaged to validate the settings. Validation may also be done via a grey-box security test (penetration test).

References:

- Vodafone Hardening Guides
- Cyber Security Testing DR
- Infrastructure Security Hardening Definition
- Generic Network Node Hardening Guideline v1
- T3 High Level Standard for TLS Hardening v1.0
- High Level Standard Mobile Device Management v1.0
- Information Classification and Protection Detailed Requirements
- CSB Control 18.2.3-C

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit | Submit

Figure 47

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 35 of 95

Vodafone Privacy Portal

ASSESSMENT AUTOMATION

k-Test 10112 In Progress 0/90 0%

2.28 Hardening Features

Unused components like software packages, applications, services, interfaces, accounts or other that are not required shall be deactivated or removed from the system.

(Ensure that everything which is not needed, will be disabled. That includes outdated interfaces or libraries, non-used system accounts, access rights, connections, etc.)

References:

- CSB Control 8.1.3
- CSB Control 12.5.1
- CSB Control 12.6.2
- CSB Control 14.2.1
- CSB Control 18.2.3.A
- CSB Control 13.1.1-H

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 48

Vodafone Privacy Portal

ASSESSMENT AUTOMATION

k-Test 10112 In Progress 0/90 0%

2.29 Patch Management

All system components shall be installed with or updated to the latest stable version with all security patches applied.

Please upload the latest Scan as evidence indicating the latest patches have been applied to the system/service/product

References:

- Security Patch Management Detailed Requirements
- Cyber Security Testing Detailed Requirements
- IT & Network Lifecycle Management Policy
- Supplier Information Security Detailed Requirements
- CSB Control 12.1.1-A

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 49

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 36 of 95

Figure 50

Figure 51

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 37 of 95

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

2.32 *Security Testing

Before go live, components shall be reviewed and may be scanned by the security team in order to check their security compliance.

API implementation / Web applications and mobile apps shall be statically tested (source code review) or penetration tested (dynamic hands on test) by an experienced penetration testing outfit.

Evidence of the testing must be attached to the control.

Type or select an option

* Explain your answer below.

Enter Reason for response here.

User & Account Management **31**

Data Protection **4**

Logging & Monitoring **9**

Data Protection (C3/C4) **1**

API Design **1**

Cloud Computing **1**

Supplier & 3rd Party **1**

Save and Exit Submit

Figure 52

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

2.33 *Security Testing

All developed source code shall be statically tested or penetration tested by an experienced penetration testing outfit.

Evidence and output of the testing must be uploaded for the control.

References:

- CSB Control 12.6.1-B

Type or select an option

Explain your answer below.

Enter Reason for response here.

User & Account Management **31**

Data Protection **4**

Logging & Monitoring **9**

Data Protection (C3/C4) **1**

API Design **1**

Cloud Computing **1**

Supplier & 3rd Party **1**

2.34 *Backup & Restore

Save and Exit Submit

Figure 53

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 38 of 95

The screenshot shows a web-based assessment tool for Vodafone's Cyber Security BSR V3. The main navigation bar includes 'ASSESSMENT AUTOMATION', 'Dashboard', 'Assessments' (Active, Archive, Recycle Bin), 'Risk Register', 'Reports', 'Setup', and 'Templates'. The current assessment is 'k-Test 10112' (In Progress). The left sidebar lists various security categories with their status (e.g., 2.31 Anti-Malware, 2.32 Security Testing, etc.). The main content area is focused on '2.34 Backup & Restore'. It asks: 'Ensure that data backup & recovery capabilities are implemented to ensure quick recovery of the availability of the service. This includes a back-up plan including which data is backed up and at which frequency. There shall be only one central backup server (or server cluster). All restore actions shall be done from a specific server under a dedicated account.' Below this are frequency options: daily, weekly, or every 6 weeks. A note states: 'In case of partial compliance, state the non-compliant point(s) from the above.' Reference links to CSB Control 12.3.1 and 12.3.2 are provided. A large text area for 'Type or select an option' is present, along with a WYSIWYG editor toolbar. A section for 'Enter Reason for response here.' is also shown. Navigation buttons (Back, Forward, Save and Exit, Submit) are at the bottom.

Figure 54

This screenshot shows the same assessment interface as Figure 54, specifically the '2.35 Backup & Restore' question. The requirement states: 'Media containing Vodafone data shall be stored in a secure environment when unattended (such as a safe or locked cabinet). When moved outside of areas which are protected by the organization's physical access controls, sensitive data on storage media must be encrypted.' It also notes: 'All electronic media that has reached the end of its lifecycle shall be disposed of in line with the "Information Media Sanitization and Disposal Detailed Guidance".' Reference links to CSB Control 8.3.1 and 8.3.2 are included. The rest of the page structure is identical to Figure 54, including the sidebar, navigation, and footer buttons.

Figure 55



5.3 User and Account Management

Questions 3.1 to 3.31

The screenshot shows the OneTrust assessment interface for Vodafone Privacy Portal. The left sidebar lists various sections like Dashboard, Assessments, Risk Register, Reports, Setup, and Templates. The main area displays an assessment titled 'k-Test 10112' which is 'In Progress'. A progress bar shows 0/90 completed. The assessment details 'Vodafone Cyber Security BSR V3'. The current section is 'Management' under 'Assessments'. The questions listed are:

- 3.1 Access
- 3.2 Access
- 3.3 Access
- 3.4 Access
- 3.5 Minimum Authentication Requirements
- 3.6 Minimum Authentication Requirements
- 3.7 User Identification and Authentication
- 3.8 User Identification & Authentication
- 3.9 User Identification & Authentication
- 3.10 User Identification and Authentication
- 3.11 User Identification & Authentication

Question 3.1 is selected and titled 'Access'. It asks: 'Non-administrative users shall only be able to access front end layers, and must not have direct access to platforms located in a different zone.' Reference: CSB Control 9.4.1. There is a text input field 'Type or select an option' and a rich text editor 'Enter Reason for response here' with a toolbar. Question 3.2 is also titled 'Access' and asks: 'If an authentication attempt is successful, the user should be informed of the date and time of their last successful log-on, and any unsuccessful log-on attempts that have happened since the last successful log-on.' Reference: Access and Authentication DR v3.0 (1.2.2.e). Question 3.3 is titled 'Access' and asks: 'Remote access shall be implemented in accordance with the Vodafone Remote Access Detailed Guidance.' Reference: [redacted].

Figure 56

This screenshot shows the continuation of the OneTrust assessment interface. The left sidebar remains the same. The current section is 'Management' under 'Assessments'. The questions listed are:

- 3.1 Access
- 3.2 Access
- 3.3 Access
- 3.4 Access
- 3.5 Minimum Authentication Requirements
- 3.6 Minimum Authentication Requirements
- 3.7 User Identification and Authentication
- 3.8 User Identification & Authentication
- 3.9 User Identification & Authentication
- 3.10 User Identification and Authentication
- 3.11 User Identification & Authentication

Question 3.2 is selected and titled 'Access'. It asks: 'If an authentication attempt is successful, the user should be informed of the date and time of their last successful log-on, and any unsuccessful log-on attempts that have happened since the last successful log-on.' Reference: Access and Authentication DR v3.0 (1.2.2.e). There is a text input field 'Type or select an option' and a rich text editor 'Enter Reason for response here' with a toolbar. Question 3.3 is also titled 'Access' and asks: 'Remote access shall be implemented in accordance with the Vodafone Remote Access Detailed Guidance.' Reference: [redacted]. Question 3.4 is also titled 'Access'.

Figure 57

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 40 of 95

The screenshot shows a web-based assessment tool. The top navigation bar includes a logo, user information, and a search bar. The main content area is titled "Vodafone Privacy Portal". On the left, a sidebar lists "ASSESSMENT AUTOMATION" sections: Dashboard, Assessments (Active, Archive, Recycle Bin), Risk Register, Reports, Setup, and Templates. Under "Assessments", there's a dropdown for "Vodafone Cyber Security BSR V3" with a "Show All Questions" option. A list of questions is displayed, starting with "Management" and then "Access". The "Access" section contains numbered points from 3.1 to 3.11. Point 3.3 is currently selected. Below each point is a brief description, a "Reference:" section with links, and a "Type or select an option" input field. A rich-text editor toolbar is above the input field. A "Save and Exit" and "Submit" button are at the bottom right.

Figure 58

This screenshot is nearly identical to Figure 58, showing the same assessment interface. The main difference is the question number: point 3.4 is now highlighted. The content of the question and its sub-points remains the same, along with the "Access" section and its requirements.

Figure 59

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

3.5 Minimum Authentication Requirements

All remote access to the Vodafone corporate network must be authenticated as follows:

- a) For users of Vodafone-issued laptops: combination of username/password, and either VPN client/digital certificate authentication from Vodafone-issued laptop or an approved alternative factor.
- b) For users of any other device type: combination of any two authentication factors.

Reference:

- Access and Authentication DR v2.0
- CSB Control 6.2.2

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 60

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

3.6 Minimum Authentication Requirements

MFA/2FA is required for:

- a) Any access to Privileged accounts which provide control over the access rights of all system users, or are able to increase their own privileges.
- b) Any access to accounts used to manage and administer cloud services (see BSR chapter 6 Cloud Computing)

Reference:

- T3 High level standard MFA Section 2.1.1 (MR2)
- Cloud Computing v2.2 (1.3.3.e)

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 61

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 42 of 95

The screenshot shows a web-based assessment tool for Vodafone Cyber Security BSR V3. The left sidebar lists various sections like Dashboard, Assessments, Active, Archive, Risk Register, Reports, Setup, and Templates. The main content area displays a test titled 'k-Test 10112' which is 'In Progress'. A question number 3.7 is highlighted. The question title is 'User Identification and Authentication'. It asks: 'Authentication factors shall be from at least two distinct types:' followed by a list of three options: a) Knowledge factors: passwords, passphrases, passcodes, PIN numbers; b) Inherent factors: fingerprint recognition, facial recognition, iris/retina recognition, voice recognition, keystroke patterns; c) Possession factors: Vodafone-issued device equipped with Vodafone digital certificate(s), hard tokens (e.g. physical token generators), soft tokens (e.g. mobile app code generators), Out-of-Band authentication (e.g. SMS single-use codes to a known number). Below the question is a reference section pointing to 'Access and Authentication DR v3.0 (2.1.1 .b)' and a text input field with a rich text editor. There is also a note to 'Explain your answer below.' with another text input field. At the bottom right are 'Save and Exit' and 'Submit' buttons.

Figure 62

This screenshot shows the same assessment interface as Figure 62, but the question number 3.7 has been changed to 3.8. The question title is now 'User Identification & Authentication'. It asks: 'When authenticating to systems and applications, the following applies:' followed by a list of two options: a) Passwords must not be displayed in clear text while being entered, transmitted and stored; b) Log-on information is being validated only on completion of all input data - if an error condition arises, the system doesn't indicate which part of the data is correct or incorrect. Below the question is a reference section pointing to 'Access and Authentication DR v3.0 (1.2.2 .b and .c)' and 'CSB Control 9.4.2' and a text input field with a rich text editor. There is also a note to 'Explain your answer below.' with another text input field. At the bottom right are 'Save and Exit' and 'Submit' buttons.

Figure 63

Figure 64

Figure 65

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 44 of 95

Figure 66

Figure 67

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 45 of 95

The screenshot shows a web-based assessment tool interface. The top navigation bar includes a logo for 'Vodafone Privacy Portal' and a user icon for 'Vodacom South Africa'. The main content area displays an assessment titled 'k-Test 10112 In Progress'. On the left, a sidebar lists various sections like 'Assessments', 'Active', 'Archive', etc. The main panel shows a question numbered 3.13 under the heading 'Management'. The question title is 'Password Policy'. The question text asks: 'Each user account shall be protected with a strong password (or other secret information known only to the user). Systems are configured to :'. It lists three points: a) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors; b) enforce the use of passwords which are compliant with the agreed password policies; and c) where technically feasible, reject previously used weak passwords, e.g. by checking against dictionaries and simple modifications of dictionary words and passwords. Below the question is a 'References:' section with a link to 'Tier 3 High Level Standard: Passwords (3.2.7), (3.2.2), (3.8.10)'. There is also a text input field labeled 'Type or select an option' and a rich text editor for 'Explain your answer below.' with a placeholder 'Enter Reason for response here.'

Figure 68

This screenshot is identical to Figure 68, showing the same assessment interface and question about Password Policy. The question text and options are the same, along with the references and the 'Explain your answer below.' section.

Figure 69

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 46 of 95

The screenshot shows a web-based assessment tool for Vodafone's Cyber Security BSR V3. The left sidebar lists various sections like Dashboard, Assessments, Active, Archive, Risk Register, Reports, Setup, and Templates. The main content area displays an assessment titled 'k-Test 10112' which is 'In Progress'. A specific question, 3.15, is highlighted under the 'Management' category. The question title is 'Password Policy'. It asks for password controls enforced by the system, listing items such as a minimum length of 8 characters, containing at least 3 of each of the following: upper case letters, lower case letters, numbers, and special characters, and being technically feasible. It also specifies that the password should not be identical to the username, different from the last 12 used passwords, and case sensitive, with a maximum password age of 90 days. Below the question is a note about partial compliance and a reference to 'Tier 3 High Level Standard: Passwords (3.8)'. There is a text input field for a reason and a rich text editor for explaining the answer.

Figure 70

This screenshot shows the continuation of the assessment in Figure 70. The next question, 3.16, is also under the 'Management' category and is titled 'Password Policy'. It states that the use of hard-coded passwords (e.g., in source code or binaries) is forbidden. The interface is identical to Figure 70, with a text input field and a rich text editor for explaining the answer. The third question, 3.17, is also under 'Management' and is titled 'Password Policy'. It states that the system shall force the user to enter their current password as well as their new password when carrying out a password change. It also refers to 'Tier 3 High Level Standard: Passwords (3.2.8)'. The layout remains consistent with the previous screens.

Figure 71

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 47 of 95

The screenshot shows a web-based assessment tool interface. The left sidebar is titled 'ASSESSMENT AUTOMATION' and includes sections for Dashboard, Assessments (Active, Archive, Recycle Bin), Risk Register, Reports, Setup, and Templates. Under 'Assessments', 'Vodafone Cyber Security BSR V3' is selected. A sub-menu for 'Management' lists several requirements, including:

- 3.1 Access
- 3.2 Access
- 3.3 Access
- 3.4 Access
- 3.5 Minimum Authentication Requirements
- 3.6 Minimum Authentication Requirements
- 3.7 User Identification and Authentication
- 3.8 User Identification & Authentication
- 3.9 User Identification & Authentication
- 3.10 User Identification and Authentication
- 3.11 User Identification &

Requirement 3.17 is currently being viewed, titled 'Password Policy'. It states: 'The system shall force the user to enter their current password as well as their new password when carrying out a password change.' Reference: 'Tier 3 High Level Standard: Passwords (3.2.8)'. There is a text input field labeled 'Type or select an option' and a rich text editor labeled 'Enter Reason for response here.'

Requirement 3.18 is also visible, titled 'Password Policy', with the note: 'Passwords shall be stored in a securely hashed form. Only algorithms specifically designed for password storage shall be used (e.g. bcrypt or PBKDF2)'.

At the bottom right are 'Save and Exit' and 'Submit' buttons.

Figure 72

This screenshot is nearly identical to Figure 72, showing the same assessment interface and requirement details. Requirement 3.18 is now the active view, titled 'Password Policy', stating: 'Passwords shall be stored in a securely hashed form. Only algorithms specifically designed for password storage shall be used (e.g. bcrypt or PBKDF2)'. Reference: 'Tier 3 High Level Standard: Passwords (3.7.1)' and 'T3 Standards on Cryptography (3.6.2)'. The text input field and rich text editor are present, along with the 'Save and Exit' and 'Submit' buttons.

Figure 73

Figure 75

Figure 76

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 49 of 95

The screenshot shows a web-based assessment tool for Vodafone's Cyber Security BSR V3. The left sidebar has a dark theme with categories like 'ASSESSMENT AUTOMATION', 'Dashboard', 'Assessments' (selected), 'Active', 'Archive', 'Recycle Bin', 'Risk Register', 'Reports', 'Setup' (selected), and 'Templates'. Under 'Assessments', there are dropdown menus for 'Show All Questions' and 'Management' (selected). A list of requirements under 'Management' includes: 3.1 Access, 3.2 Access, 3.3 Access, 3.4 Access, 3.5 Minimum Authentication Requirements, 3.6 Minimum Authentication Requirements, 3.7 User Identification and Authentication, 3.8 User Identification & Authentication, 3.9 User Identification & Authentication, 3.10 User Identification and Authentication, and 3.11 User Identification &. Requirement 3.21 is currently selected, titled 'Account Management'. It states: 'The system shall provide the capability to deactivate or suspend accounts either manually or automatically given some predefined criteria are met (i.e. period of inactivity, company leaver, user has changed role)'. Reference points to 'Access and Authentication DR v3.0 (1.4.2.d and 1.4.2.e)' and 'CSB Control 9.2.6.A'. Below this is a text input field with placeholder 'Type or select an option' and a rich text editor with toolbar icons. Requirement 3.22 follows, also titled 'Account Management', with the instruction: 'The channels for providing users with their username and their initial or reset password shall be different from one-another.' Reference points to 'Tier 3 High Level Standard: Passwords (3.3.1)'. Below this is another text input field with placeholder 'Enter Reason for response here' and a rich text editor.

Figure 77

This screenshot is identical to Figure 77, showing the same assessment task for 'Account Management' (Requirement 3.21). The interface, requirements list, and text input fields are all the same.

Figure 78

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

3.23 *Account Management

Details of all access requests and approvals must be logged and retained for audit purposes, including any emergency access requests.
Logs must clearly indicate the level (access rights) and extent (which systems) of access requested.

Reference:
 • Access and Authentication DR v3.0 (1.4.1.a)
 • CG8 Control 9.2.2

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 80

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

3.24 *Account Management

All users should be authenticated using a unique identifier (such as Vodafone managed identity) and an authenticator (password, passphrase, passcode or PIN) before they can gain access to corporate electronic resources.

Reference:
 • Tier 3 High Level Standard: Passwords (3.1.1)

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 81

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 51 of 95

The screenshot shows a web-based assessment tool for Vodafone's Cyber Security BSR V3. The left sidebar has a dark theme with navigation options like Dashboard, Assessments, Active, Archive, Risk Register, Reports, Setup, and Templates. The main content area is titled 'k-Test 10112 In Progress' and shows progress '0/90' and '0%'.

Section 3.25: Account Management

If the use of shared accounts (used by multiple individuals) is necessary, this requires formal approval, documentation and the assignment of a responsible owner. Mechanisms and processes shall be in place which:

- a) restrict the ability to use a shared account to only those users who need it to perform their role.
- b) remove the ability to use a shared account in a timely manner when users who have been authorised to use it change their role or leave the organisation.
- c) The use of shared accounts must be linked to the user's identity at all times, with logging enabled to identify misuse.

References:

- Access and Authentication DR v3.0 (1.1.5.d)
- CSB Control 9.2.1-A

Section 3.26: Account Management

If appropriate, users must have no more than two simultaneous sessions to the same system.

Reference:

- Access and Authentication DR v3.0 (1.2.2.f)

Section 3.27: Account Management

Privileged access must:

- a) only be granted on a need-to-use basis for a specific, narrowly defined purpose, and should be granted on an event-by-event basis where possible.
- b) must only be assigned to accounts separate to those used for users' day-to-day

Buttons at the bottom right include 'Save and Exit' and 'Submit'.

Figure 82

The screenshot shows the same web-based assessment tool as Figure 82. The left sidebar and main header are identical.

Section 3.26: Account Management

If appropriate, users must have no more than two simultaneous sessions to the same system.

Reference:

- Access and Authentication DR v3.0 (1.2.2.f)

Section 3.27: Account Management

Privileged access must:

- a) only be granted on a need-to-use basis for a specific, narrowly defined purpose, and should be granted on an event-by-event basis where possible.
- b) must only be assigned to accounts separate to those used for users' day-to-day

Buttons at the bottom right include 'Save and Exit' and 'Submit'.

Figure 83

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 52 of 95

Vodafone Privacy Portal

ASSESSMENT AUTOMATION

k-Test 10112 In Progress 0/90 0%

3.27 *Account Management

Privileged access must

- a) only be granted on a need-to-use basis for a specific, narrowly defined purpose, and should be granted on an event-by-event basis where possible.
- b) must only be assigned to accounts separate to those used for users' day-to-day activities, but these accounts and access rights must still be linked to the user's primary identity
- c) all access to, and use of, privileged accounts must be logged.

Reference:

- Access and Authentication DR v2.0
- CSB Control 9.2.3

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 84

Vodafone Privacy Portal

ASSESSMENT AUTOMATION

k-Test 10112 In Progress 0/90 0%

3.28 *Account Management

User identities and user access rights shall be reviewed and documented on a regular basis (no more than 3 calendar months) and upon change of a user's role to confirm that they continue to be still required. Identities and access found to be inappropriate or no longer required needs to be adjusted/removed in a timely manner.

If any unauthorised privileged access is identified, this must be blocked immediately.

Reference:

- Access and Authentication DR v3.0 (1.4.2.d)
- CSB Control 9.2.5

Type or select an option

* Explain your answer below.

Enter Reason for response here.

3.29 *Account management

Save and Exit Submit

Figure 85

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 53 of 95

The screenshot shows a web-based assessment tool for Vodafone. The left sidebar has sections like Dashboard, Assessments, Active, Archive, Risk Register, Reports, Setup, and Templates. Under Assessments, 'Vodafone Cyber Security BSR V3' is selected. A sub-menu for 'Management' lists questions 3.1 through 3.11. Question 3.29 is currently displayed, titled '*Account management'. It asks: 'The user's line manager is responsible to ensure users' identities, accounts and access rights are'. Below this is a list of requirements: a) blocked within 30 calendar days after their last working day and b) deleted within 6 months after their last working day. Data required for audits or investigations may be retained. c) There must be an emergency leaver process which allows the immediate blocking of user accounts in high risk scenarios if jointly approved by the user's line manager, HR and security teams. d) These requirements also apply to users who cancel their employment with Vodafone on or before their start date. A 'Reference:' section lists 'Access and Authentication DR v3.0 (1.4.2.e)' and 'CSB Control 9.2.6.A'. There is a text input field 'Type or select an option' and a rich text editor 'Enter Reason for response here.' with a toolbar. Navigation buttons (Back, Forward, Save and Exit, Submit) are at the bottom.

Figure 86

This screenshot shows the same assessment interface as Figure 86. The left sidebar and 'Management' sub-menu are identical. Question 3.30 is now displayed, titled '*Functional Accounts'. It asks: 'Where the use of functional accounts (used by systems / applications) is necessary for business or operational reasons, this requires a formal approval, documentation and the assignment of a responsible system owner. Potential use of functional accounts for unauthorised use by an individual must be monitored.' A 'Reference:' section lists 'CSB Control 9.2.1-A'. A text input field 'Type or select an option' and a rich text editor 'Enter Reason for response here.' with a toolbar are present. Navigation buttons (Back, Forward, Save and Exit, Submit) are at the bottom. Below this question, the next one, 3.31, is partially visible with the title '*Functional Accounts'.

Figure 87

The screenshot shows a web-based assessment tool interface. At the top, there's a red header bar with the text "Vodafone Privacy Portal". Below it, a left sidebar titled "ASSESSMENT AUTOMATION" lists various navigation options like Dashboard, Assessments, Active, Archive, Risk Register, Reports, setup, and Templates. The main content area displays an assessment task titled "k-Test 10112 In Progress". A progress bar indicates 0/90 completed at 0%. The task itself is titled "3.31 Functional Accounts" and includes a detailed description: "Functional accounts (accounts used by scripts and processes) shall use secure authentication methods. Where passwords are used for authentication of functional accounts, very strong passwords shall be used (a minimum of 14 random characters)". It also lists a reference: "Tier 3 High Level Standard: Passwords (3.6.1)". There's a text input field labeled "Type or select an option" and a rich text editor toolbar. A note says "Enter Reason for response here." At the bottom right, there are "Save and Exit" and "Submit" buttons.

Figure 88

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 55 of 95



5.4 Data Protection

Questions 4.1 to 4.4

4.1 ***Data Integrity & Input Controls**
System critical data shall be transmitted along with checksums using strong hash functions to ensure data integrity during transmission.
Reference:
• CSB Control 13.2.1
Type or select an option
* Explain your answer below.
Enter Reason for response here.

4.2 ***Data Integrity & Input Controls**
All operations that modify data (e.g. update, delete, insert) shall ensure that no intermediate stage in the operation that can lead to data integrity problems. Either the operation is fully completed or fully incomplete.

Figure 89

4.2 ***Data Integrity & Input Controls**
All operations that modify data (e.g. update, delete, insert) shall ensure that no intermediate stage in the operation that can lead to data integrity problems. Either the operation is fully completed or fully incomplete.

4.3 ***Data Integrity & Input Controls**
All processes that receive data input (both manual and automated) shall control and validate input data in terms of formatting, length and syntax.

Figure 90

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 56 of 95

The screenshot shows a web-based assessment tool for Vodafone's Cyber Security BSR V3. The left sidebar lists categories like Dashboard, Assessments, Active, Archive, Recycle Bin, Risk Register, Reports, Setup, and Templates. The main content area shows a section titled '4.3 Data Integrity & Input Controls' with a question about processes receiving data input. Below it is another section '4.4 Data Integrity & Input Controls' with a question about legal banners. A large red banner at the top right indicates the user is part of 'Vodafone South Africa'.

Figure 91

This screenshot is identical to Figure 91, showing the same section of the Vodafone Privacy Portal. It displays the '4.3 Data Integrity & Input Controls' and '4.4 Data Integrity & Input Controls' sections, both of which include questions about legal banners and proposed legal language. The red 'Vodafone South Africa' banner is present in the top right corner.

Figure 92

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT		
Document Number: V1 Title: SPDA How to Guideline	Revision: 2	Owner: Kally Mabe Page 57 of 95



5.5 Logging and Monitoring

Questions 5.1 to 5.9

5.1 ***Logging & Monitoring**

The following events shall be logged at each level:

- a) successful logins (log-in and out)
- b) failed login attempts
- c) privilege escalation attempts (e.g. switch user on privileged accounts)
- d) rejected connections
- e) violations of access restrictions
- f) manipulation attempts (e.g. shutdown of the system, modification of system time)
- g) creation or modification of user accounts
- h) access to the security logs
- i) attempts to modify the security policy

In case of partial compliance, state the non-compliant point(s) from the above.

Reference:

- Logging and Monitoring DR v2.4 FINAL
- CSB Control 12.4.1

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 93

5.2 ***Logging & Monitoring**

The following details must be provided with each logged event:

- a) time
- b) date
- c) type of event
- d) IP address of the origin
- e) MSISDN of the origin
- f) user ID

In case of partial compliance, state the non-compliant point(s) from the above.

Reference:

- Logging and Monitoring DR v2.4 FINAL
- CSB Control 12.4.1

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 94

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 58 of 95

Figure 95

Figure 96

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 59 of 95

The screenshot shows the OneTrust platform interface for Vodafone's Privacy Portal. The top navigation bar includes the OneTrust logo, a search bar, and user account information. The main content area is titled 'Vodafone Privacy Portal' and shows an assessment titled 'k-Test 10112' which is currently 'In Progress' with 0/90 questions completed. The left sidebar has a dark theme and lists several sections: Dashboard, Assessments (Active, Archive, Recycle Bin, Risk Register), Reports, Setup, and Templates. Under 'Assessments', there is a dropdown menu for 'Vodafone Cyber Security BSR V3' which contains sections like Security Hygiene & Essentials (26 questions), User & Account Management (31 questions), Data Protection (44 questions), and Logging & Monitoring (9 questions). The main content area displays section 5.5 'Logging & Monitoring' with a question about read-only access to logging systems. It includes a 'References' section pointing to 'Logging and Monitoring DR v2.4 FINAL'. Below this is a rich text editor with a toolbar and a placeholder 'Enter Reason for response here.' Section 5.6 follows, also related to Logging & Monitoring.

Figure 97

This screenshot shows the continuation of the assessment from Figure 97. The main content area now displays section 5.6 'Logging & Monitoring' with a question about audit log configuration. It includes a 'References' section pointing to 'Logging and Monitoring DR v2.4 FINAL' and 'CSB Control 12.4.3'. Below this is a rich text editor with a toolbar and a placeholder 'Enter Reason for response here.' Section 5.7 follows, also related to Logging & Monitoring.

Figure 98

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

Assessment Automation

- Dashboard
- Assessments
 - Active
 - Archive
 - Recycle Bin
 - Risk Register
 - Reports
- Setup
- Templates

5.7 **Logging & Monitoring**

The log system shall provide the capability to:

* a) select events that took place within a specific time range.
* b) select combinations of events.
* c) select events where a specific user used a particular privilege.

In case of partial compliance, state the non-compliant point(s) from the above.

References:

- Logging and Monitoring DR v2.4 FINAL
- CSB Control 12.4.1
- CSB Control 12.4.3

Type or select an option

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 99

Vodafone Privacy Portal

k-Test 10112 In Progress 0/90 0%

Assessment Automation

- Dashboard
- Assessments
 - Active
 - Archive
 - Recycle Bin
 - Risk Register
 - Reports
- Setup
- Templates

5.8 **Logging & Monitoring**

The system shall provide the means to detect and alarm unauthorised or improper use of the system by comparing events against pre-defined expected behaviour.

References:

- Logging and Monitoring DR v2.4 FINAL
- CSB Control 12.4.1
- CSB Control 12.4.3

Type or select an option

* Explain your answer below.

Enter Reason for response here.

5.9 **Logging & Monitoring**

Save and Exit Submit

Figure 100

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 61 of 95

The screenshot shows a web-based assessment tool interface. At the top, there's a red header bar with the text "Vodafone Privacy Portal". Below it, a left sidebar titled "ASSESSMENT AUTOMATION" lists various sections: Dashboard, Assessments (Active, Archive, Recycle Bin), Reports, setup, and Templates. Under "Assessments", a dropdown menu is open, showing "Vodafone Cyber Security BSR V3" and options to "Show All Questions" or "Show by Category". The main content area displays a task titled "5.9 Logging & Monitoring". The task description states: "An automated process shall be implemented to send log files or defined log events to a security log server." It includes a "References:" section with links to "Logging and Monitoring DR v2.4 FINAL" and "CSB Control 13.1.1-A" through "J". There's also a "Type or select an option" input field and a "Save and Exit" button at the bottom.

Figure 101

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 62 of 95



5.6 Data Protection {C3/C4}

Question 6.1

6.1 * Does the project process, store and/or transfer personal data, C3 or C4 data?

Yes No

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 102

5.7 API Design

Question 7.1

7.1 * Does the solution provide or access an API(s) either internally or externally using HTTP-based interfaces such as SOAP, REST, or JSON?

Yes No

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 103

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 63 of 95



5.8 Cloud Computing

Question 8.1

The screenshot shows the OneTrust Privacy, Security & Compliance platform interface for Vodafone. The left sidebar lists various assessments under 'ASSESSMENT AUTOMATION'. The main area displays question 8.1: 'Is the solution partially or fully hosted in a cloud?'. It includes a 'Yes' or 'No' button, a rich text editor for explanation, and a 'Save and Exit' or 'Submit' button.

8.1 *Is the solution partially or fully hosted in a cloud?
If Yes is selected you will be redirected to answer the questions relating to Cloud.
If No is selected you will be redirected to the next section.

Yes No

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 104

5.9 Web Application

Question 9.1

The screenshot shows the OneTrust Privacy, Security & Compliance platform interface for Vodafone. The left sidebar lists various assessments under 'ASSESSMENT AUTOMATION'. The main area displays question 9.1: 'Is any 3rd party company involved in one or more of the following activities?'. It lists five options: development, maintenance/operations, integration, testing, and support. It includes a 'Yes' or 'No' button, a rich text editor for explanation, and a 'Save and Exit' or 'Submit' button.

9.1 *Is any 3rd party company involved in one or more of the following activities:

1. -development
2. -maintenance/operations
3. -integration
4. -testing
5. -support

Yes No

* Explain your answer below.

Enter Reason for response here.

Save and Exit Submit

Figure 105

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 64 of 95



5.10 Web Application Security

Question 10.1

The screenshot shows the OneTrust Privacy, Security & Governance platform. The URL is https://app-eu.onetrust.com/assessment/details/21da44b9-7f3c-4b07-961c-80219724baf6. The title bar says "OneTrust | Privacy, Security & G..." and "Vodafone Privacy Portal". The main content area displays an assessment titled "k-Test 10112 In Progress". On the left, there's a sidebar with "ASSESSMENT AUTOMATION" and "Assessments" selected. Under "Assessments", "Active" is chosen, showing a list of categories: Security Hygiene & Essentials (26), User & Account Management (31), Data Protection (4), Logging & Monitoring (4), Data Protection (C3/C4) (4), API Design (1), Cloud Computing (4), Supplier & 3rd Party (1), Web Application Security (1), Mobile Security (1), VOIP (1), and CPE (4). The "Web Application Security" category is highlighted with a red border. The main content area shows a question "10.1 *Web Application Security" with the sub-instruction "Does the project include any Web Based applications?". There are "Yes" and "No" buttons. Below the buttons is a text area with the placeholder "Enter Reason for response here." and a rich text editor toolbar. At the bottom right are "Save and Exit" and "Submit" buttons.

Figure 106

5.11 Mobile Security

Question 11.1

The screenshot shows the OneTrust Privacy, Security & Governance platform. The URL is https://app-eu.onetrust.com/assessment/details/21da44b9-7f3c-4b07-961c-80219724baf6. The title bar says "OneTrust | Privacy, Security & G..." and "Vodafone Privacy Portal". The main content area displays an assessment titled "k-Test 10112 In Progress". On the left, there's a sidebar with "ASSESSMENT AUTOMATION" and "Assessments" selected. Under "Assessments", "Active" is chosen, showing a list of categories: Security Hygiene & Essentials (26), User & Account Management (31), Data Protection (4), Logging & Monitoring (4), Data Protection (C3/C4) (4), API Design (1), Cloud Computing (4), Supplier & 3rd Party (1), Web Application Security (1), Mobile Security (1), VOIP (1), and CPE (4). The "Mobile Security" category is highlighted with a red border. The main content area shows a question "11.1 *Mobile Application Security" with the sub-instruction "Does the project include the development or usage of mobile applications?". There are "Yes" and "No" buttons. Below the buttons is a text area with the placeholder "Enter Reason for response here." and a rich text editor toolbar. At the bottom right are "Save and Exit" and "Submit" buttons.

Figure 107

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 65 of 95



5.12 Monitoring & Logging

Question 12.1

The screenshot shows the Vodafone Privacy Portal interface. On the left, there's a navigation sidebar with options like Dashboard, Assessments, Active, Archive, Recycle Bin, Risk Register, Reports, Setup, and Templates. Under Assessments, 'Vodacom Cyber Security BSR V3' is selected, showing a list of questions with their respective scores. The main area displays Question 12.1: "12.1 * Does the product deal with Voice over IP or with Unified Communications?". It includes a 'Yes' button, a 'No' button, and a text area for explanation with rich text editing tools. At the bottom right are 'Save and Exit' and 'Submit' buttons.

Figure 108

5.13 CPE

Question 13.1

The screenshot shows the Vodafone Privacy Portal interface. The navigation sidebar is identical to Figure 108. The main area displays Question 13.1: "13.1 * Does the project deal with Customer Premise Equipment?". It includes a 'Yes' button, a 'No' button, and a text area for explanation with rich text editing tools. At the bottom right are 'Save and Exit' and 'Submit' buttons.

Figure 109

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe
Page 66 of 95

Title: SPDA How to Guideline



5.14 Technical Assurance

Question 14.1 to 14.2

14.1 *CMDB
Has the systems/applications in scope been updated on CMDB/CIA portals with the relevant evidence?
Yes No
* Explain your answer below.
Enter Reason for response here.

14.2 *Business Continuity Management
Has the system been integrated with the BCM (Business Continuity Management) processes?
i.e.- It has a BCM rating, TRP (Technical Recovery Plan), etc?
Yes No
* Explain your answer below.
Enter Reason for response here.

Figure 110

14.1 *CMDB
Has the systems/applications in scope been updated on CMDB/CIA portals with the relevant evidence?
Yes No
* Explain your answer below.
Enter Reason for response here.

14.2 *Business Continuity Management
Has the system been integrated with the BCM (Business Continuity Management) processes?
i.e.- It has a BCM rating, TRP (Technical Recovery Plan), etc?
Yes No
* Explain your answer below.
Enter Reason for response here.

Figure 111

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 67 of 95



5.15 End of Assessment

Question 15.1

The screenshot shows a web browser window for the OneTrust Privacy, Security & Compliance platform. The title bar reads "OneTrust | Privacy, Security & C..." and the URL is "https://app-eu.onetrust.com/assessment/details/21da44b9-7f3c-4b07-961c-80219724bfb6". The main header "Vodafone Privacy Portal" is displayed, along with a user icon and a dropdown menu for "Vodafone South Africa". The left sidebar is titled "ASSESSMENT AUTOMATION" and includes sections for "Dashboard", "Assessments" (with "Active", "Archive", and "Recycle Bin" options), "Risk Register", "Reports", "setup", and "Templates". Under "Assessments", there is a dropdown menu set to "Show All Questions". A list of assessment categories is shown with their respective scores: User & Account Management (31), Data Protection (44), Logging & Monitoring (9), Data Protection (C3/C4) (1), API Design (1), Cloud Computing (1), Supplier & 3rd Party (1), Web Application Security (1), Mobile Security (1), VOIP (1), CPE (1), Technical Assurance (2). A section titled "End of Technology Security Assessment" contains instructions: "To fully complete the assessment and send it for review to the Cyber Security Team, please ensure that the submit button is clicked." It also notes: "If the Submit button is greyed out and you are not able to click it, please check the assessment and ensure that all required questions are answered and the relevant evidence is uploaded." A message at the bottom says "Thank you for adhering to the SPDA process." At the bottom right are "Save and Exit" and "Submit" buttons. The status bar at the top indicates "k-Test 10112 In Progress 0/90 0%".

Figure 112

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 68 of 95



6. OneTrust: How to Raise a Risk

Click on the Risk Register in the panel on the left

The screenshot shows the OneTrust Risk Register interface. On the left, there's a navigation sidebar with options like Dashboard, Assessments (Active, Archive, Recycle Bin), Reports, Setup, and Templates. The 'Risk Register' option is highlighted with a yellow box and has a yellow arrow pointing to it from below. The main area is titled 'Risk Register' and shows a table of risks. The columns include ID, Risk Name, Risk Template, Description, Residual Risk Level, Residual Risk Score, Organization, and Source. There are 20 rows of data, with the last row showing a red 'X' icon. At the bottom, there's a pagination bar showing 'Showing 1 - 20 of 10166'.

Figure 113

The CSO then selects the 'Add Risk' in blue on the top right of the screen

This screenshot is identical to Figure 113, showing the OneTrust Risk Register page. A yellow arrow points from the top right of the screen to the 'Add Risk' button, which is highlighted with a yellow box. The rest of the interface, including the sidebar and the risk register table, is the same as in Figure 113.

Figure 114

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 69 of 95



The CSO select the 'Create New Risk' radial button

The screenshot shows the 'Create Risk' page of the Vodafone Privacy Portal. On the left, there's a sidebar with 'ASSESSMENT AUTOMATION' and 'Assessments' selected. The main area has a title 'Create New Risk' and a sub-instruction 'Please fill out the fields below to create a risk'. There are two radio buttons: 'Select a Risk From the Library' (unchecked) and 'Create New Risk' (checked). Below these is a section titled 'Select a Risk' with a dropdown menu. At the bottom are 'Previous', 'Cancel', 'Create', and 'Next' buttons.

Figure 115

The 'Create New Risk' box will be displayed

This screenshot shows the expanded 'Create New Risk' form. The 'Create New Risk' radio button is selected. The form includes fields for 'Organization' (dropdown), 'Inherent Risk Level' (dropdown with a red square icon), 'Risk Name' (text input with character count 0/300), 'Category' (dropdown), 'Risk Owners' (dropdown with placeholder 'Please select Risk Owner'), 'Risk Approver' (dropdown with placeholder 'Please select approver'), 'Deadline' (date picker), and 'Reminder' (checkbox). At the bottom are 'Previous', 'Cancel', 'Create', and 'Next' buttons.

Figure 116

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 70 of 95



The CSO will then have to complete the fields raised

Create Risk

Please fill out the fields below to create a risk

Select a Risk From the Library
 Create New Risk

Organization
Vodacom South Africa

Inherent Risk Level
20 Likelihood: Likely (51% to 80%)
Impact: Very High

Risk Name
Test 10111 10 / 300

Category
Availability

Risk Owners
Please select Risk Owner
Kesh Munillal

Risk Approver
Please select approver
Kesh Munillal

Previous Cancel Create Next

Figure 117

Create Risk

Risk Approver
Please select approver
Kesh Munillal

Deadline
8/25/2022, 00:00

Reminder
6

Description
Demo Risk 9 / 4000

Treatment Plan
Remediate Risk 14 / 4000

Show More Details

Previous Cancel Create Next

Figure 118

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 71 of 95



Then the CSO will select the 'Next' button in blue at the bottom right of the screen

The screenshot shows the 'Create Risk' form in the Vodafone Privacy Portal. The 'Risk Approver' field is set to 'Kesh Munillal'. The 'Deadline' is set to '8/25/2022, 00:00'. The 'Reminder' field has a value of '6'. The 'Description' field contains the text 'Demo Risk'. The 'Treatment Plan' field contains 'Remediate Risk'. At the bottom right of the form, there are three buttons: 'Cancel', 'Create', and 'Next'. The 'Next' button is highlighted with a yellow box.

Figure 119

The Add Controls page is displayed. The CSO then selects the 'Add Control' blue button in the middle of the screen

The screenshot shows the 'Add Controls' page in the Vodafone Privacy Portal. The page title is 'Add Controls'. In the center, there is a graphic of a document with a plus sign. Below the graphic is a blue button labeled 'Add Controls'. Underneath the button, the text 'No Items to Display' is visible. At the bottom right of the page, there are three buttons: 'Cancel', 'Create', and 'Next'. The 'Next' button is highlighted with a yellow box.

Figure 120

The CSO will need to select the 'Add Control' button

The 'Add Control' box will be displayed

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 72 of 95

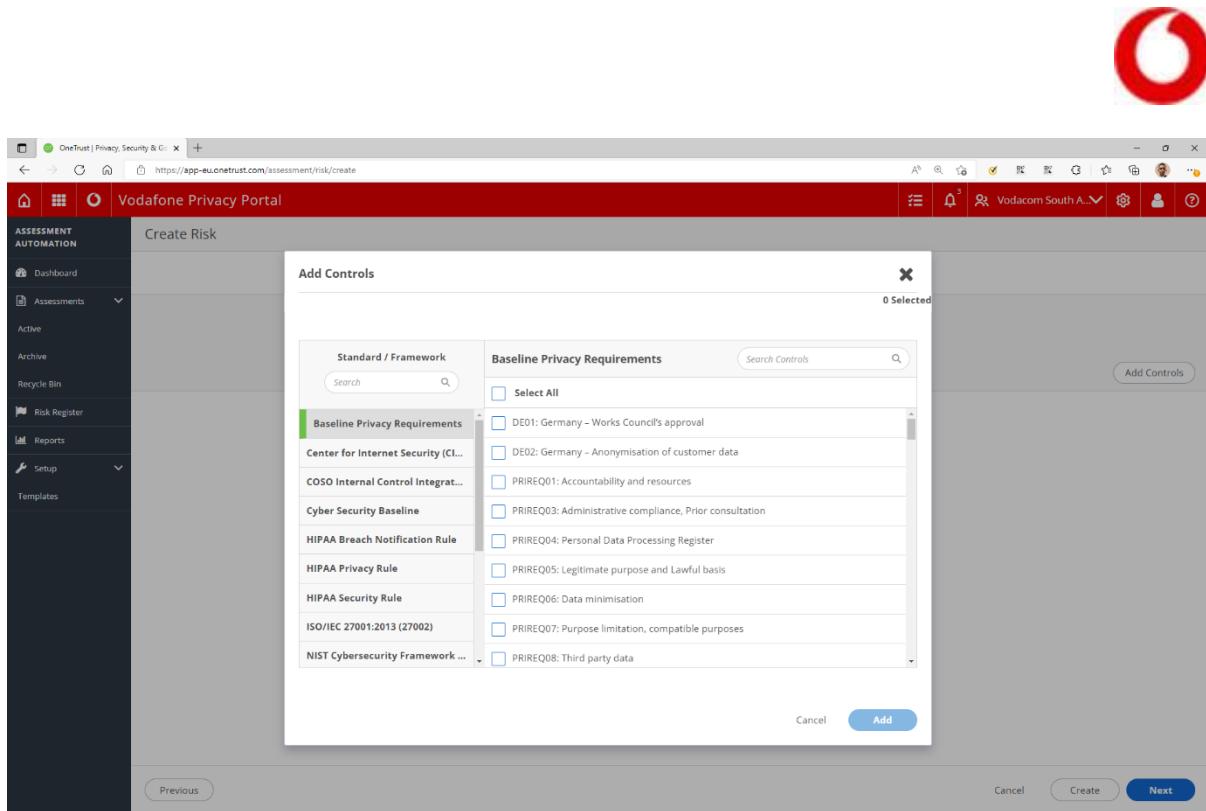


Figure 121

Select the 'Cyber Security Baseline' option displayed under the 'Standard / Framework' and then select the applicable control and select 'Add'

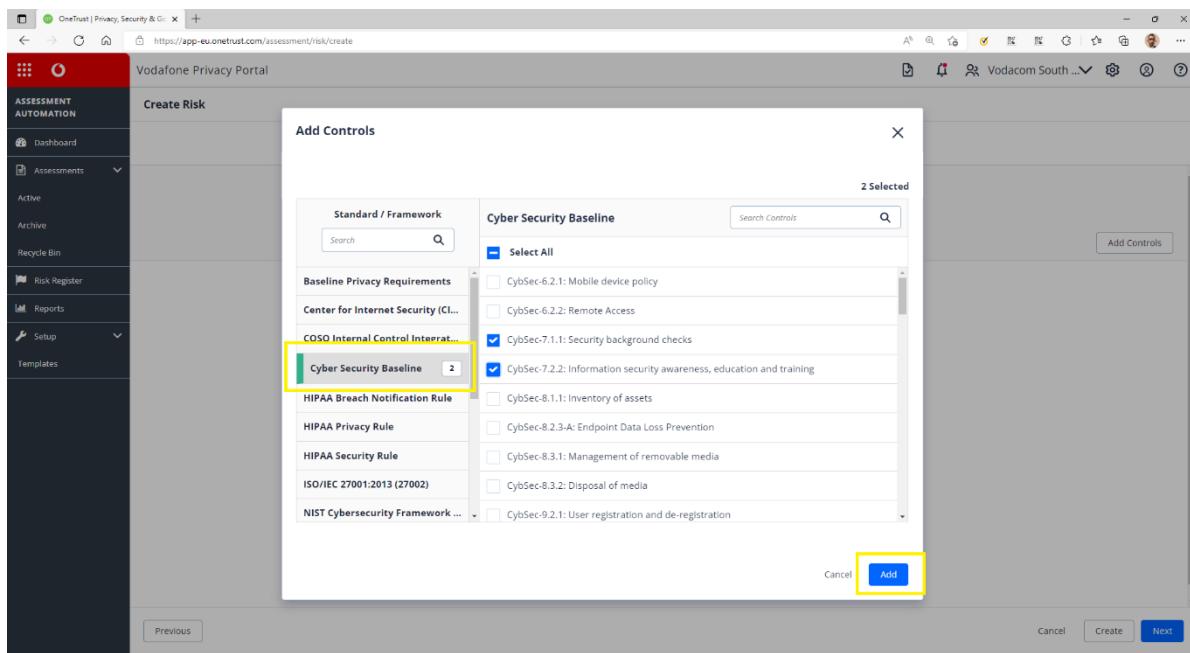


Figure 122

An email will automatically be sent to the Risk Approver, as below. Click on the 'View Risk' button

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 73 of 95

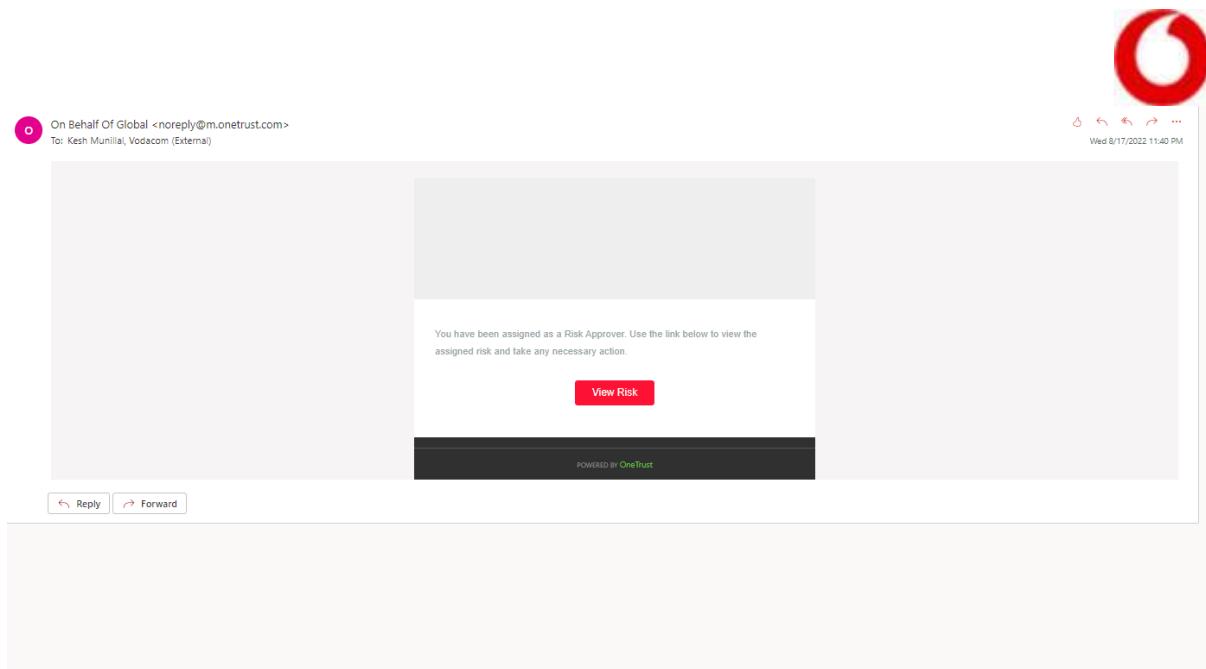


Figure 123

The CSOs are then able to select the 'View Risk' button in the email or select the Risk Register in OneTrust and the Risk will be displayed

ID	Risk Name	Risk Template	Description	Residual Risk Level	Residual Risk Score	Organization	Source
123425	Test 10111	----	Demo Risk	High	20	Vodacom South Africa	----
123405	PA Supplier Data Processing (High)	----	PA Supplier Data Processing Su...	High	20	Vodacom South Africa	SOB 2.0 USSD Journey for Premiu...
123404	PA Number of Data Subjects (Low)	----	PA Number of Data Subjects <2...	Low	7	Vodacom South Africa	SOB 2.0 USSD Journey for Premiu...
123403	PA Nature of Data (Medium)	----	PA Nature of Data Account dat...	Medium	15	Vodacom South Africa	SOB 2.0 USSD Journey for Premiu...
123402	PA Hosting Environment (Medium)	----	PA Hosting Environment Third ...	Medium	8	Vodacom South Africa	SOB 2.0 USSD Journey for Premiu...
123401	PA Purpose of processing (High)	----	PA Purpose of processing CRM ...	High	22	Vodacom South Africa	SOB 2.0 USSD Journey for Premiu...
123391	PA Number of Data Subjects (High)	----	PA Number of Data Subjects >=...	High	22	Vodacom South Africa	Ex VAT call charges on low value c...
123390	PA Nature of Data (High)	----	PA Nature of Data Authenticati...	High	22	Vodacom South Africa	Ex VAT call charges on low value c...
123389	PA Purpose of processing (Medium)	----	PA Purpose of processing Cust...	Medium	15	Vodacom South Africa	Ex VAT call charges on low value c...
123388	PA Nature of Data (Low)	----	PA Nature of Data Basic compa...	Low	7	Vodacom South Africa	Test Austin
123387	Vodacom South Africa	SACS Access Report Fraud Risk ...
123378	PA Supplier Data Processing (High)	----	PA Supplier Data Processing Su...	High	20	Vodacom South Africa	Shop N Save Product DLS VLive...
123377	PA Hosting Environment (Low)	----	PA Hosting Environment Local ...	Low	1	Vodacom South Africa	Shop N Save Product DLS VLive...
123376	PA Purpose of processing (Medium)	----	PA Purpose of processing Cust...	Medium	15	Vodacom South Africa	Shop N Save Product DLS VLive...
123375	PA Purpose of processing (Medium)	----	PA Purpose of processing Cust...	Medium	15	Vodacom South Africa	Shop N Save Product DLS VLive...
123367	PA Nature of Data (Medium)	----	PA Nature of Data Account dat...	Medium	15	Vodacom South Africa	Enhance Order Validation rules S...

Figure 124



The Risk is displayed

This screenshot shows the OneTrust Privacy, Security & Compliance platform interface for the Vodafone Privacy Portal. The main title bar reads "OneTrust | Privacy, Security & C..." and the URL is "https://app-eu.onetrust.com/assessment/risk-details/0f66290f-7bec-4712-9755-4e2a6661ec4e/summary". The left sidebar has sections for ASSESSMENT AUTOMATION, Dashboard, Assessments (Active, Archive, Recycle Bin), Risk Register, Reports, Setup, and Templates. The main content area is titled "Risk Details" under "Risk Register > 123425". It shows the "IDENTIFIED" stage guidance: "In the Identified stage, the identified risk is in an open state and requires further review." Below this are sections for "Key Risk Information", "Residual Risk Level" (20 - Likelihood: Likely (51% to 80%) / Impact: Very High), "Risk Name" (Test 10111), "Risk Owners" (Kesh Munillal), "Risk Approver" (Kesh Munillal), and "Treatment Status" (----). The top navigation bar includes tabs for IDENTIFIED, EVALUATION, TREATMENT, MONITORING, and ADVANCE. The ADVANCE tab is highlighted. The main content area has tabs for Summary, Details, History, Tasks, Controls, and More. The "Assigned to Me" section shows 0 items. The "Related" section also shows 0 items.

Figure 125

The CSO's are then able to select the 'Advance' button and work through the Risk as per the screenshots below

This screenshot is identical to Figure 125, showing the OneTrust Privacy, Security & Compliance platform interface for the Vodafone Privacy Portal. The main title bar and URL are the same. The left sidebar and main content area are identical, including the "IDENTIFIED" stage guidance, "Key Risk Information" section, and the "ADVANCE" tab being highlighted. The "Assigned to Me" and "Related" sections are both showing 0 items.

Figure 126

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 75 of 95



The Risk will be moved along to ‘Evaluate’

Risk Details
Risk Register > 123425

ASSESSMENT AUTOMATION

IDENTIFIED EVALUATION TREATMENT MONITORING

Stage Guidance

Evaluation

In the Evaluation stage, the scoring and quantification is set based on the level of risk observed by the business. As the risk approver, you can outline the treatment plan and controls required to be implemented by the risk owner. If treatment is not needed, you can advance the workflow to the Monitoring stage.

Key Risk Information

Residual Risk Level
20 - Likelihood: Likely (51% to 80%) / Impact: Very High

Risk Name
Test 10111

Risk Owners
Kesh Munillal

Risk Approver

Assigned to Me 0

No Items to Display

Object Show Open Items. Task... Search...

Related 0

Object Asset, Entity, Processin... Search...

Figure 127

Once the CSO has evaluated the Risk and is ready to move forward, they will select the ‘Advance’ button

Advance Stage

Please confirm Risk Owner and Treatment Plan. The Risk Owner will receive a notification that there is a risk that needs to be mitigated.

* Risk Owner
Please select Risk Owner
Kesh Munillal

* Treatment Plan
Remediate Risk

Cancel Save & Advance

Object Asset, Entity, Processin... Search...

Figure 128

The CSO will be prompted to save the Risk and advance

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 76 of 95



The screenshot shows the OneTrust interface within the Vodafone Privacy Portal. On the left, there's a sidebar with options like 'Assessment Automation', 'Dashboard', 'Assessments' (Active, Archive, Recycle Bin), 'Risk Register', 'Reports', 'Setup', and 'Templates'. The main area is titled 'Risk Details' under 'Risk Register > 12345'. A modal window titled 'Advance Stage' is open, containing a green circular icon with a checkmark. It asks to confirm the Risk Owner and Treatment Plan. The 'Risk Owner' field is populated with 'Kesh Munillai'. The 'Treatment Plan' field contains 'Remediate Risk'. At the bottom right of the modal is a blue 'Save & Advance' button, which is highlighted with a yellow box.

Figure 129

The Risk Owner will receive the following mail once you have selected the ‘Save and Advance’ button. The Risk Owner may then select the ‘Review Risk’ button in the email

The screenshot shows an email message. The header indicates it's from 'On Behalf Of Global <noreply@m.onetrust.com>' to 'Kesh Munillai, Vodafone (External)' at 'Wed 8/17/2022 11:47 PM'. The subject line is 'You have been assigned as a Risk Owner'. The body of the email contains a message: 'You have been assigned as a Risk Owner. Use the link below to view the assigned risk and respond to the approvers Treatment Plan. You can also update any controls as necessary.' Below this is a red 'View Risk' button. At the bottom of the email, there's a black bar with 'POWERED BY OneTrust'. Below the email are standard reply and forward buttons.

Figure 130

When a Treatment Plan (also referred to the Risk Remediation Plan or Control Improvement Plan) is put in place, the CSO will receive a mail to review the Treatment Plan

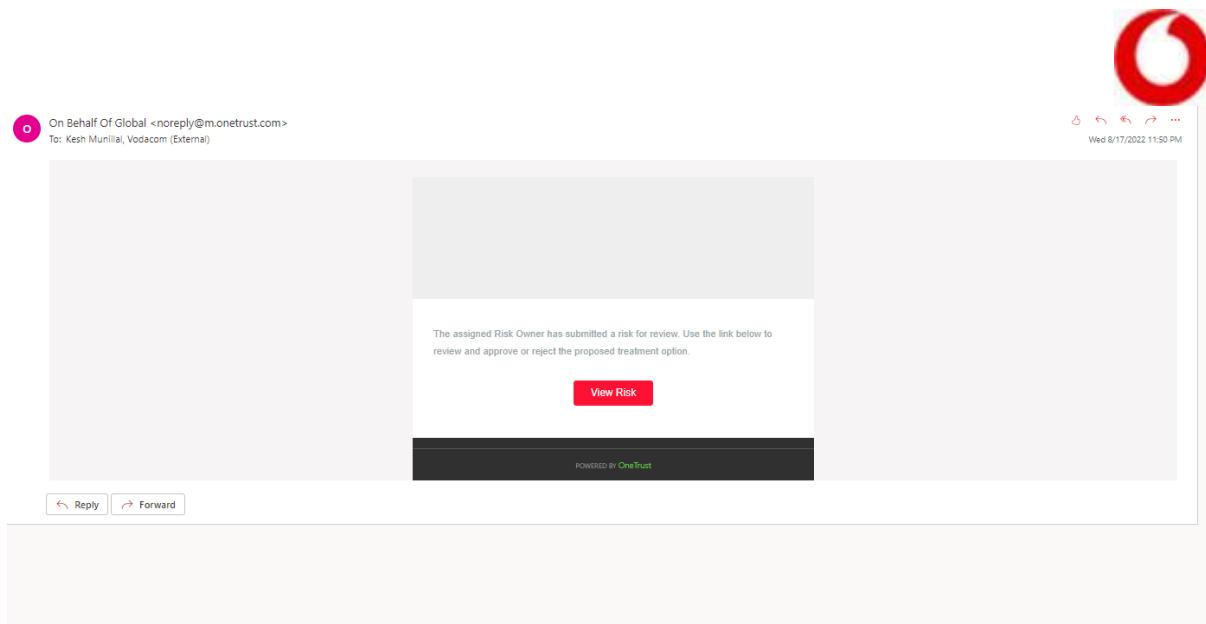


Figure 131

The CSO then selects the blue 'Submit' button at the top right of the screen

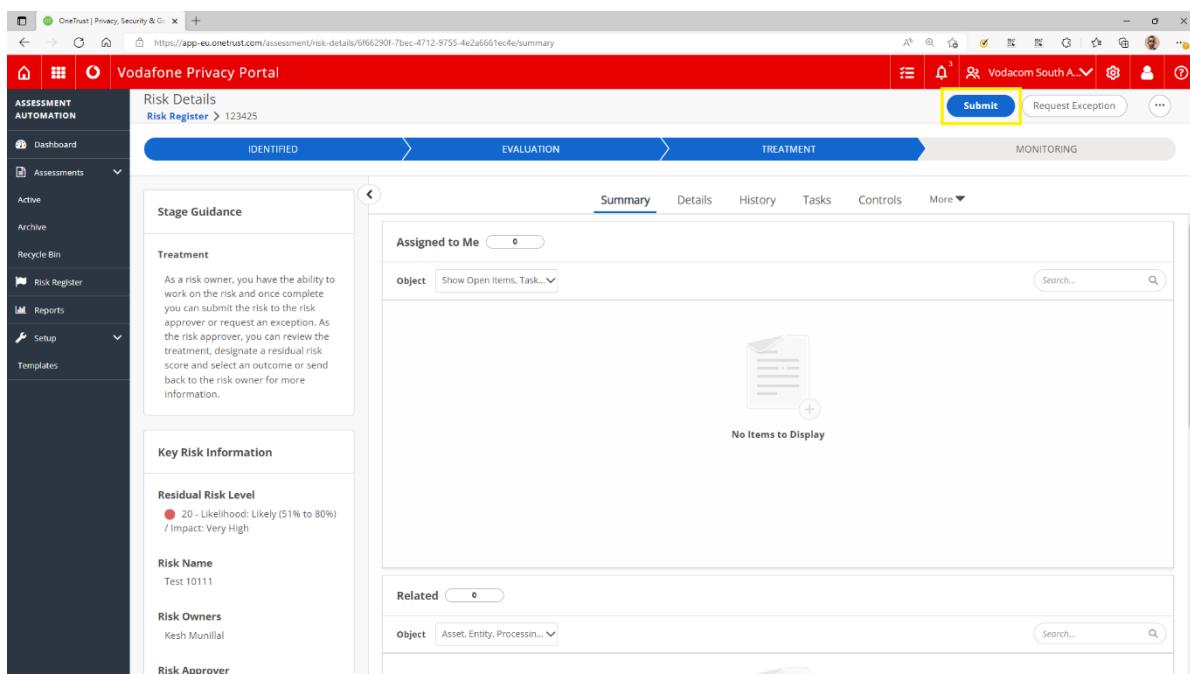


Figure 132

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT



The 'Submit Treatment Plan' box will be displayed

A screenshot of the Vodafone Privacy Portal. On the left, there's a sidebar with 'ASSESSMENT AUTOMATION' and 'Assessments' selected. Under 'Assessments', options like 'Active', 'Archive', 'Recycle Bin', 'Risk Register', 'Reports', 'Setup', and 'Templates' are listed. The main area shows 'Risk Details' for 'Risk Register > 123425'. A horizontal navigation bar at the top has tabs for 'IDENTIFIED', 'EVALUATION', 'TREATMENT' (which is highlighted in blue), and 'MONITORING'. A 'Treatment' section contains 'Stage Guidance' and 'Key Risk Information' (Residual Risk Level: 20 - Likelihood: Likely (51% to 80%), Impact: Very High). Below this are fields for 'Risk Name' (Test 10111), 'Risk Owners' (Kesh Munillal), and 'Risk Approver'. A central modal window titled 'Submit Treatment Plan' contains a green checkmark icon, a message asking 'Are you sure you wish to submit this treatment for review?', a 'Comments' input field, and a 'Submit' button. The background shows a 'Tasks' section with a search bar.

Figure 133

Select the blue 'Submit' button

The CSO then may Approve the Treatment Plan

A screenshot of the Vodafone Privacy Portal, similar to Figure 133 but with a different view. The 'TREATMENT' tab is still selected. The 'Treatment' section now shows 'Assigned to Me' with a count of 0. The 'Object' dropdown is set to 'Show Open Items, Task...'. A large central area displays a document icon with the message 'No Items to Display'. The top right of the screen has a toolbar with icons for 'Approve' (highlighted in yellow), 'Send Back', and '...'.

Figure 134

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe
Page 79 of 95

Title: SPDA How to Guideline



The CSO captures the required information and selects the blue 'Confirm' button

Vodafone Privacy Portal

Risk Details
Risk Register > 123425

Approve Risk

Stage Guidance

Treatment

Key Risk Information

Residual Risk Level

Risk Name

Risk Owners

Risk Approver

Result: Accepted

Residual Risk Level / Score: 20 (Likelihood: Likely (51% to 80%) / Impact: Very High)

Comments: Low Risk

Cancel Confirm

Figure 135

Vodafone Privacy Portal

Risk Details
Risk Register > 123425

Approve Risk

Stage Guidance

Treatment

Key Risk Information

Residual Risk Level

Risk Name

Risk Owners

Risk Approver

Result: Accepted

Residual Risk Level / Score: 20 (Likelihood: Likely (51% to 80%) / Impact: Very High)

Comments: Low Risk

Cancel Confirm

Figure 136

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe

Title: SPDA How to Guideline

Page 80 of 95

The screenshot shows the OneTrust Privacy, Security & Governance platform. The URL is https://app-eu.onetrust.com/assessment/risk-details/0f66290f-7bec-4712-9755-4e2a6661ec4e/summary. The page title is "Vodafone Privacy Portal". The left sidebar has sections for ASSESSMENT AUTOMATION (Dashboard, Assessments, Active, Archive, Recycle Bin, Risk Register, Reports, Setup, Templates). The main content area shows "Risk Details" for Risk Register ID 123425. It includes tabs for IDENTIFIED, EVALUATION, TREATMENT (highlighted in blue), and MONITORING. The TREATMENT tab has sub-sections: Stage Guidance (Monitoring), Key Risk Information, Residual Risk Level (20 - Likelihood: Likely (51% to 80%) / Impact: Very High), Risk Name (Test 10111), Risk Owners (Kesh Munillal), Risk Approver (Kesh Munillal), and Treatment Status (Approved). A yellow box highlights the "Approved" button.

Figure 137

The screenshot shows an email message. The recipient is Kesh Munillal. The subject line is "Risk Treatment Approved". The message body starts with "A risk treatment has been approved. Use the link below to view the risk." followed by "Comments by Kesh Munillal: "Low Risk"" and a "View Risk" button. At the bottom, there is a "Powered by OneTrust" footer. The "View Risk" button is highlighted with a yellow box.

Figure 138



6.1 Risk Register

ID	Risk Name	Risk Template	Description	Residual Risk Level	Residual Risk Score	Organization	Source
123425	Test 10111	----	Demo Risk	High	20	Vodacom South Africa	-----
123405	PA Supplier Data Processing (High)	----	PA Supplier Data Processing Su...	High	20	Vodacom South Africa	SOB 2.0 USSD Journey for Freemu...
123404	PA Number of Data Subjects (Low)	----	PA Number of Data Subjects <2...	Low	7	Vodacom South Africa	SOB 2.0 USSD Journey for Freemu...
123403	PA Nature of Data (Medium)	----	PA Nature of Data Account dat...	Medium	15	Vodacom South Africa	SOB 2.0 USSD Journey for Freemu...
123402	PA Hosting Environment (Medium)	----	PA Hosting Environment Third ...	Medium	8	Vodacom South Africa	SOB 2.0 USSD Journey for Freemu...
123401	PA Purpose of processing (High)	----	PA Purpose of processing CRM ...	High	22	Vodacom South Africa	SOB 2.0 USSD Journey for Freemu...
123391	PA Number of Data Subjects (High)	----	PA Number of Data Subjects >=...	High	22	Vodacom South Africa	Ex VAT call charges on low value c...
123390	PA Nature of Data (High)	----	PA Nature of Data Authentificati...	High	22	Vodacom South Africa	Ex VAT call charges on low value c...
123389	PA Purpose of processing (Medium)	----	PA Purpose of processing Cust...	Medium	15	Vodacom South Africa	Ex VAT call charges on low value c...
123388	PA Nature of Data (Low)	----	PA Nature of Data Basic compa...	Low	7	Vodacom South Africa	Test Austin
123387	-----	----	-----	-----	-----	Vodacom South Africa	SACS Access Report Fraud Risk ...
123378	PA Supplier Data Processing (High)	----	PA Supplier Data Processing Su...	High	20	Vodacom South Africa	Shop N Save Product DLS VLive...
123377	PA Hosting Environment (Low)	----	PA Hosting Environment Local ...	Low	1	Vodacom South Africa	Shop N Save Product DLS VLive...
123376	PA Purpose of processing (Medium)	----	PA Purpose of processing Cust...	Medium	15	Vodacom South Africa	Shop N Save Product DLS VLive...
123375	PA Purpose of processing (Medium)	----	PA Purpose of processing Cust...	Medium	15	Vodacom South Africa	Shop N Save Product DLS VLive...
123367	PA Nature of Data (Medium)	----	PA Nature of Data Account dat...	Medium	15	Vodacom South Africa	Enhance Order Validation rules S...

Figure 139

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 82 of 95



7. Decommissioning

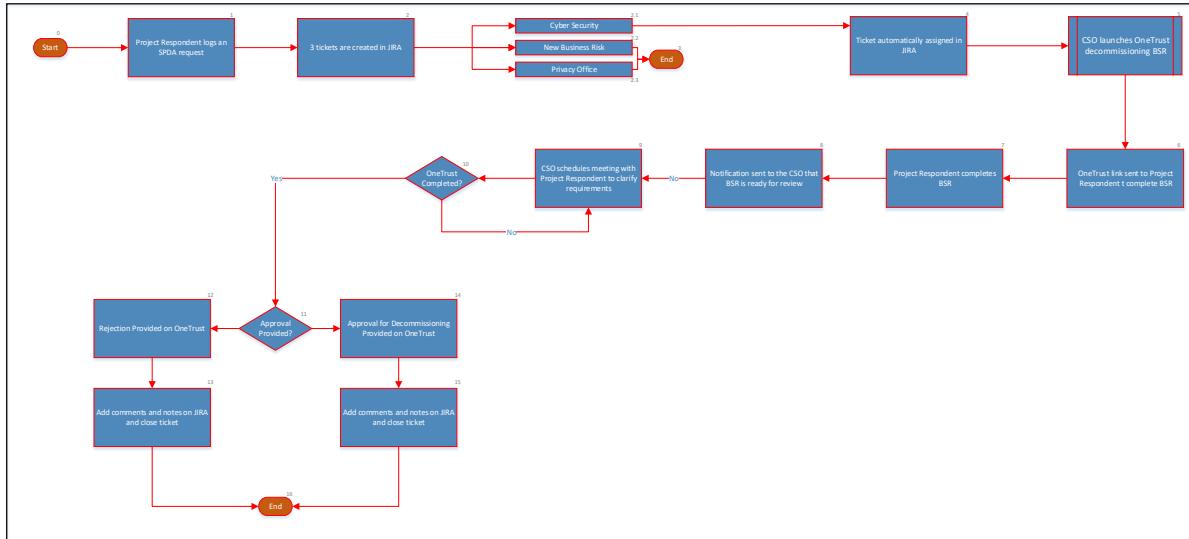


Figure 140

- 7.1 An SPDA is initiated by the Project Respondent logging a 'Feature' in JIRA and answering the mandatory questions for PI initiatives, or by completing the Initial Qualifying Questionnaire Template in Confluence, depending on whether you have a project logged in JIRA or not for the decommissioning
- 7.2 There are 3 tickets that will then be created in JIRA, one on each of the Kanban boards, Cyber Security, Privacy, and Business Risk. The 3 areas are required to sign off on the tickets to close the request. The three tickets should have the following items attached:
 - Remedy ticket – screenshot
 - CMDB screenshot (before and after)
 - AWS - if it's Cloud, confirmation from the Cloud team that the account is decommissioned
 - Architecture design - if it's a partial decommissioning
- 7.2.1 The Cyber Security Ticket is created in JIRA
- 7.2.2 The New Business Risk Ticket is created in JIRA
- 7.2.3 The Privacy ticket is created in JIRA
- 7.3 For purposes of this document, we will only detail the Cyber Security ticket further, and thus, the other processes that are mentioned continue further in their respective areas documents, however, will not be detailed further in this document
- 7.4 The Cyber Security ticket is auto assigned, and an email is automatically generated and sent to the CSO to whom the ticket has been assigned
- 7.5 The responsible CSO then launches an assessment on the OneTrust system. The CSO logs into the OneTrust system and launches an assessment, by selecting the Assessment Automation tile, and then clicking on the Launch Assessment button in the top right-hand corner of the screen. The CSO then selects the 'VSA Technology Security Decommissioning assessment' tile
- 7.6 OneTrust then sends an automated email to the Project Respondent with a link to a questionnaire that is to be completed by the Project Respondent
- 7.7 The Project Respondent completes the OneTrust assessment and submits the completed questionnaire on the OneTrust system
- 7.8 The OneTrust system then sends the CSO a notification email to let them know that the BSR has been completed by the Project Respondent and is ready to be reviewed

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT



7.9 The CSO will then review the OneTrust assessment and schedule a meeting with the Project Respondent for a walk-through of the product or service and to review the OneTrust report that was submitted by the Project Respondent

7.10 Once the OneTrust assessment has been completed successfully, the process moves on

7.11 From the OneTrust assessment, the CSO will either provide an approval or rejection of the project/development

7.12 Should the project/development be rejected, the rejection is recorded on OneTrust

7.13 Comments are added to JIRA regarding the rejection and the ticket is closed. The process then continues to point 6.19

7.14 In the case that the project/development is approved, the approval is recorded on OneTrust

7.15 Comments are added to JIRA and the ticket is closed

7.16 The process ends

The complete process is attached below.



Decommissioning
process.vsdx



Decommissioning
process.pdf

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT		
Document Number: V1 Title: SPDA How to Guideline	Revision: 2	Owner: Kally Mabe Page 84 of 95



8. OneTrust: Launch Decommissioning Assessment

You will be able to view the assessments that have been sent out to the Business, and you are also able to launch an assessment from here

The screenshot shows the OneTrust interface for the Vodafone Privacy Portal. The left sidebar includes 'ASSESSMENT AUTOMATION' with 'Dashboard', 'Assessments' (which is selected), 'Risk Register', 'Reports', 'Setup', and 'Templates'. The main content area is titled 'Assessments' and shows a table of 2704 assessments. The columns include ID, Name, Stage, Result, Residual Risk Level, Residual Risk Score, Organization, Respondent, Approver, Deadline, and Op. Several assessments are listed with their status (e.g., Not Started, Under Review, In Progress). The 'Launch Assessment' button is located at the top right of the main content area.

Figure 141

To launch an assessment, the CSO will select the 'Launch Assessment' button

This screenshot is identical to Figure 141, showing the OneTrust interface for the Vodafone Privacy Portal. The 'Assessments' tab is selected in the sidebar. A yellow arrow points to the 'Launch Assessment' button at the top right of the main content area. The table below lists 2704 assessments with various details like ID, Name, Status, and Respondent.

Figure 142

The 'VSA Technology Security Decommissioning assessment' is selected

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe
Page 85 of 95

Title: SPDA How to Guideline

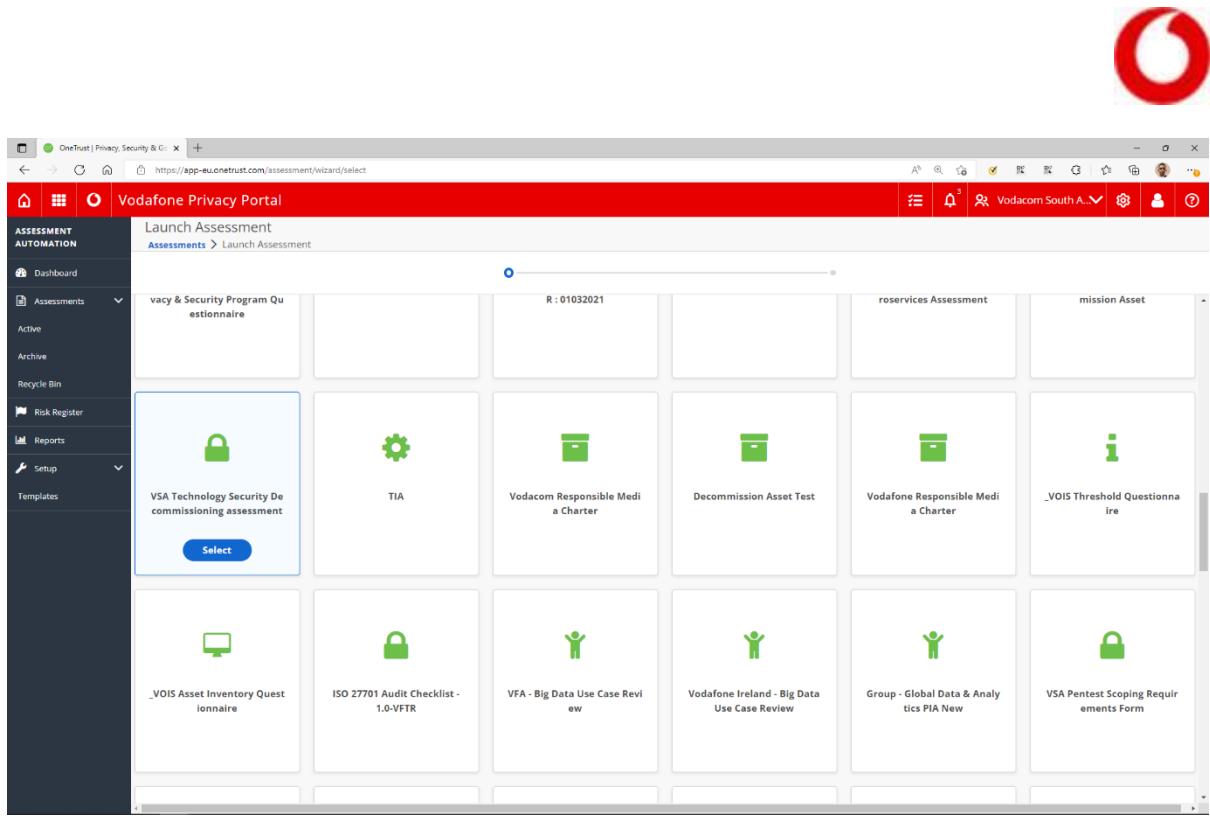


Figure 143

The CSO will complete the editable boxes, 'Name', 'Approver', and 'Respondent'. The 'Organisation' field will already contain 'Vodacom South Africa'. If it is a different organization, this field needs to be changed. Then select the 'Launch' button (bottom right of screen). This will enable One-trust to send an email with a link to the OneTrust assessment to the Project Respondent for completion.

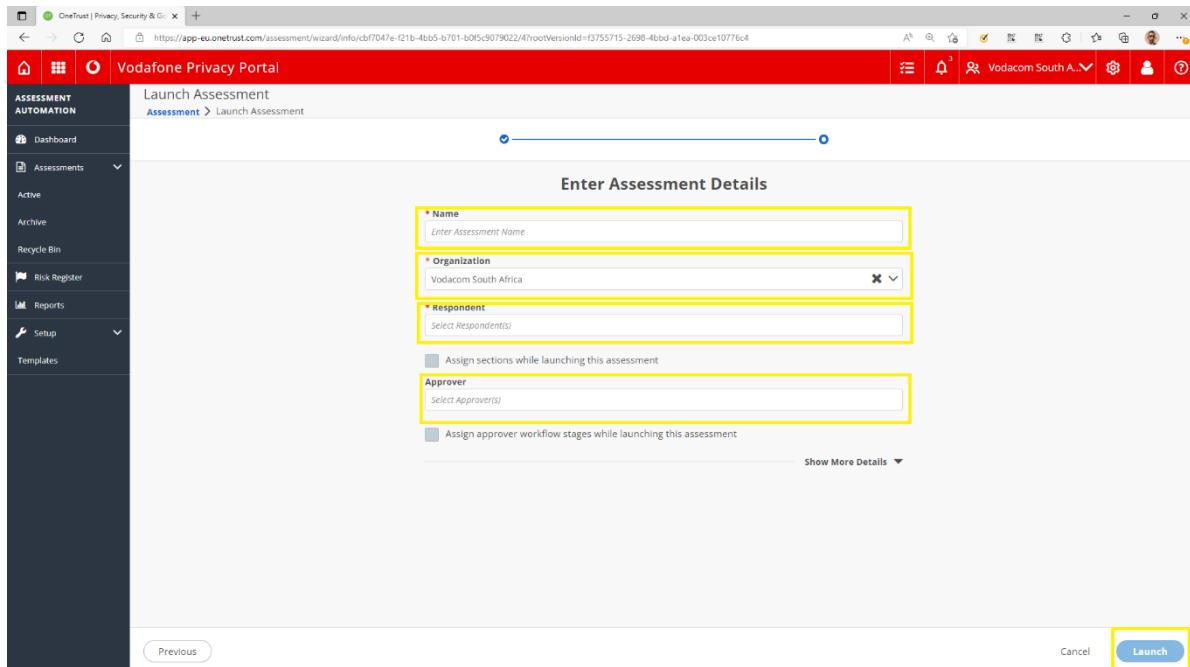


Figure 144

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 86 of 95



9. OneTrust: Cyber Security Assessment - Decommissioning

9.1 Select Stakeholder and Project Info

Questions 1.1 to 1.5

The screenshot shows the OneTrust Vodafone Privacy Portal interface. On the left, a sidebar lists various assessment sections: Dashboard, Assessments (Active, Archive, Recycle Bin, Risk Register), Reports, Setup, and Templates. The main area displays a 'VSA Technology Security Decommissioning assessment' titled 'Demo for Audit'. The status is 'Not Started' with 0/13 questions completed at 0%. The first question, 1.1, asks for the service/product name to be decommissioned, with a rich text editor and a note to enter the answer here. The second question, 1.2, asks for Remedy or Jira Number associated with the decommissioning, also with a rich text editor. The third question, 1.3, asks for the decommissioning date, which is a date picker field. The fourth question, 1.4, asks for Business Owner details, with a rich text editor. The fifth question, 1.5, asks for the Project Lead associated with the project, with a rich text editor. A 'Submit' button is located at the bottom right.

Figure 145

This screenshot continues from Figure 145. It shows the same portal interface with the 'VSA Technology Security Decommissioning assessment' and 'Demo for Audit' title. The status remains 'Not Started' with 0/13 questions completed at 0%. The third question, 1.3, is now visible, asking for the decommissioning date, represented by a date picker field. The fourth question, 1.4, is also visible, asking for Business Owner details, with a rich text editor. The other questions (1.1, 1.2, 1.5) are still present in the sidebar. A 'Submit' button is located at the bottom right.

Figure 146

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Revision: 2

Owner: Kally Mabe
Title: SPDA How to Guideline
Page 87 of 95



OneTrust | Privacy, Security & Compliance

Vodafone Privacy Portal

Demo for Audit Not Started 0/13 0% ...

ASSESSMENT AUTOMATION

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

VSA Technology Security Decommissioning assessment

Show All Questions

Welcome

Stakeholders and Project Information * 4 >

1.1 Please provide the service / product name that will be decommissioned

1.2 Please provide Remedy or Jira Number associated with the decommissioning

1.3 Please indicate the decommissioning date

1.4 Please provide the Business Owner details

1.5 Please provide the Project Lead associated with the project

Project / Service Information * 2 >

Decommissioning requirements * 6 >

1.4 *Please provide the Business Owner details

Enter your answer here.

1.5 Please provide the Project Lead associated with the project

Enter your answer here.

Submit ...

Figure 147

9.2 Project/Service Information

Questions 2.1 to 2.2

OneTrust | Privacy, Security & Compliance

Vodafone Privacy Portal

Demo for Audit Not Started 0/13 0% ...

ASSESSMENT AUTOMATION

Dashboard

Assessments

Active

Archive

Recycle Bin

Risk Register

Reports

Setup

Templates

VSA Technology Security Decommissioning assessment

Show All Questions

Welcome

Stakeholders and Project Information * 4 >

Project / Service Information * 2 >

2.1 *Please provide a brief overview of what is the service that is being decommissioned

Enter your answer here.

2.2 *Please attach design/product description documents for the solution.

This question requires an attachment

Enter your answer here.

Decommissioning requirements * 6 >

End of Assessment >

2.1 *Please provide a brief overview of what is the service that is being decommissioned

Enter your answer here.

2.2 *Please attach design/product description documents for the solution.

This question requires an attachment

Enter your answer here.

Submit ...

Figure 148

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 88 of 95



9.3 Decommissioning Requirements

Questions 3.1 to 3.6

The screenshot shows the OneTrust Privacy, Security & Governance platform interface for Vodafone. The left sidebar is titled 'ASSESSMENT AUTOMATION' and includes 'Dashboard', 'Assessments' (selected), 'Active', 'Archive', 'Recycle Bin', 'Risk Register', 'Reports', 'Setup' (selected), and 'Templates'. Under 'Assessments', 'Decommissioning requirements' is selected. The main content area displays two questions:

3.1 *Please indicate the process to be followed for the Disposal of the hardware and the data on the system
Evidence of the process must also be provided.
NB: To verify the appropriate methodologies for disposal please refer to the standards [T2 High Level Standard Information Sanitisation and Disposal v1.2*](#) - Technology Standard Template (sharepoint.com)

3.2 *Backups of the service/system
Please indicate if the backups of the system will be kept or disposed off. Please indicate the reason for the response below and provide the relevant evidence .
Yes No

Figure 149

The screenshot shows the OneTrust Privacy, Security & Governance platform interface for Vodafone. The left sidebar is identical to Figure 149. The main content area displays two questions:

3.3 *Please provide evidence that any associated ARM groups related to the service/server are removed.
Yes No
Explain your answer below.
Enter Reason for response here.

3.4 *Please indicate that all routing and firewall rules have been removed or will be removed and provide the relevant evidence thereof.
Yes No
Explain your answer below.
Enter Reason for response here.

Figure 150

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 89 of 95

The screenshot shows a web-based assessment portal for Vodafone. The left sidebar has a dark theme with navigation options like Dashboard, Assessments (Active, Archive, Recycle Bin), Risk Register, Reports, Setup, and Templates. Under Assessments, 'VSA Technology Security Decommissioning assessment' is selected. The main area displays a form titled 'Demo for Audit' with a progress bar at 0/13 and 0% completion. The form contains several questions:

- 3.5 System/service removal from Asset management system.** A question asking for evidence that a system/service is removed from CMDB or a ticket logged for the removal of assets. It includes 'Yes' and 'No' buttons and a note about evidence.
- 3.6 Please provide the approved Change Request for the decommissioning activity?** A rich text editor for entering the change request.

At the bottom right are back/forward buttons and a blue 'Submit' button.

Figure 151

9.4 End of Assessment

Question 4.1

The screenshot shows the same assessment portal. The left sidebar now shows 'End of Assessment' under the 'Assessments' section. The main area displays a summary of the completed assessment:

- 4.1 End of Technology Security Assessment**
- A note: 'To complete the assessment and send it for review to the Technology Security Team, please ensure that the submit button is clicked.'
- If the submit button is greyed out, it says: 'If the Submit button is greyed out and you are not able to click it, please double check the assessment and ensure that all required questions are answered and the relevant evidence is uploaded.'
- A thank you message: 'Thank you for adhering to the SPDA process.'

At the bottom right are back/forward buttons and a blue 'Submit' button.

Figure 152

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1
Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 90 of 95



10. Risk Definition and Prioritisation

What Defines the Risk/Complexity and therefore prioritization of tickets			
Low	Medium	High	Critical
No new systems or interfaces introduced.	New internal interfaces introduced.	New external interfaces introduced.	New hosting environment and/or network introduced. (Public Cloud)
Only minor configuration changes to existing systems.	Single new internal system introduced.	New internet facing system introduced.	New remote access solution and/or non-standard remote access requirements.
Existing approved supplier using existing remote access method.	Existing approved supplier changing to a new approved remote access method.	Multiple new internal systems introduced.	SOX/ PCI DSS impacts.
Low ZA impact changes already assessed by Group Cyber Security.	No SOx, PCI DSS impacts.	New supplier using an approved remote access method.	Customer facing system.
No SOx, PCI DSS impacts.	Employee data but no Customer data.	SOx impacts.	Involves C4 data.
Low Impact changes to 3 rd party provided services that have already been assessed by Supplier Security (Cyber GRC).	Infrastructure projects	Involves Customer data and/or sensitive business data.	Regulatory.
		Regulatory	Internet facing Systems
		Time to Gate2<1 month	Customer mobile apps
		P\PCI Information	
What potential impacts on Security will project have? Minimum Requirements to Go Live			
No engagement. Send advice notes	Baseline Security Requirements (BSR) self-assessment by Security Champion.	Baseline Security Requirements (BSR) assessment by SbD.	Baseline Security Requirements (BSR) assessment by SbD.
Waiver of Baseline Security Requirements (BSR).		HLD review	HLD review / LLD review
CCS SCAN	CCS SCAN	CCS SCAN	OneTrust\VRM
VA SCAN	VA SCAN	VA SCAN	VA SCAN
Security tooling installed	WAS SCAN	WAS SCAN	WAS SCAN
Patching	Security tooling installed	Security tooling installed	PEN TEST before go-live
Whitesource SCA scans for Dev	Patching	Patching	No critical findings
	Whitesource SCA scans for Dev	Whitesource SCA scans for Dev, SAST	Whitesource SCA scans for Dev, SAST, DAST
PenTesting Requirement			
No PenTest Requirement	PenTesting will be catered for in the event it falls part of the mission critical asset annual testing	PenTesting to be completed prior to go Live	PenTesting to be completed prior to go Live
Remediation Requirements			
All Baseline Assurance to be compliant prior introduction into production.	Remediation as per Findings related to policy	Remediation as per Findings related to policy	Remediation as per Findings related to policy

Figure 153

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT



11. Definitions:

11.1 **Project Respondent:** An individual logging a request in JIRA

11.2 **BSR:** Baseline Security Requirements – An in-depth security assessment

11.3 **PI:** A Program Increment (PI) is a timebox during which an Agile Release Train (ART) delivers incremental value in the form of working, tested software and systems

11.4 **Initial Qualifying Questionnaire:** A set of questions posed at the outset of the process followed to log an SPDA request. The answers to these questions will determine if a full BSR is required to be completed

11.5 **JIRA:** Program/project logging and monitoring tool used by Vodacom to record and track progress of initiatives

11.6 **OneTrust:** Privacy Management Software Platform used to support the organization to adhere to compliance and audit requirements

11.7 **Vulnerability Scans:** A tool by organisations to monitor their networks, systems, and applications for security vulnerabilities

11.8 **Risk Remediation Plan:** The process of strategically prioritizing corrective efforts so that security risks are addressed

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe

Page 92 of 95



12. Roles and Responsibilities

The following teams must have input into the successful project approval.

12.1 Cyber Security Officer:

The Cyber Security Officer is a technical cyber security expert, one or more cyber security officers are assigned from the Cyber Secure by Design team to Business Units. The designated CSO's will work with project stakeholders to consult, review the design and architecture, facilitate technical security testing, identify project risks and make remediation recommendations from inception until the approval or rejection of the project

The CSO works with the Business Units to develop a remediation plan that is acceptable to minimize the risks and move forward with the development or deployment. Planning and scoping of Penetration Tests form part of a CSO's roles and responsibilities.

12.2 Security Architecture:

The architecture team, together with the designated CSO is required to review system design, identify gaps and risks and provide guidance in line with Vodafone/Vodacom policies and standards and applicable good practices. Security Architecture and CSO approval are required for the design of a product or service.

12.3 Cyber Defense:

The cyber defense team is responsible for Privilege Identity and access management compliance of the project, Penetration Testing, Vulnerability Management, Security Monitoring, CSANS, and reporting of the system vulnerabilities and configuration weaknesses.

They are responsible for sharing CSANS with product owners to remediate within specific timelines. Cyber defense is also responsible for actioning notices from Vodafone.

12.4 GRC:

The GRC team is responsible for Governance, Risk, and Compliance. They assist with Cyber Security audit preparation and support and remediate gaps.

The GRC team is responsible for 3rd party vendor assessments based on the CSB controls.

They ensure that the Vodacom South Africa policies are aligned with Vodafone policies.

Policy Dispensations and RACS are also part of the GRC team's responsibilities.

The GRC team designs and delivers cyber security awareness communications and phishing simulations to the business, as well as Risk initiatives.

12.5 New Business Risk

New Business Risk Management is the process of a new multi-disciplinary process of identifying risks during the new product and service development lifecycle using the Vodacom Risk Methodology. This includes the identification, measurement, and evaluation of risks and the implementation of controls to mitigate and control risks.

12.6 Application Technical Team

An Application Technical Team is typically a set of individuals who have the specific skill set that helps develop products or services within Vodacom. The team is responsible for the technical development associated with the project. The team may consist of Vodacom staff and/or external vendors.

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe
Page 93 of 95



13. Supporting documents / Policies

#	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 Process Manual	Vodacom South Africa Cyber Security
13	Policy Dispensation and Security Risk Assessment Requirements	PD and SRA Requirements - Vodacom 2021-11-17.pptx (sharepoint.com)

14. Document history

Revision	Date	Changes	Other affected documents	Approved by
1	16/04/2021	First published version	None	Christopher Knox
1	13/10/2022	Updated to incorporate New JIRA Demand process and updated formatting	SPDA Process Manual	Christopher Knox

UNCONTROLLED IF PRINTED OR REPRODUCED IN ANY FORMAT

Document Number: V1

Title: SPDA How to Guideline

Revision: 2

Owner: Kally Mabe

Page 94 of 95