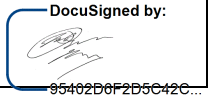
Doc No. V5	SPDA How to Guideline			Rev. 2
Applicable areas of business: Vodacom SA		Responsible Division Technology Security (Darshan Lakha -EHOD)		
Approval	Name	Job Title/ Role	Signature	Date
Content Owner	Kally Mabe	Senior CSO – 2IC		15/10/2022
Approved by	Christopher Knox	Manager: Cyber Security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

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

1. SPDA Procedure

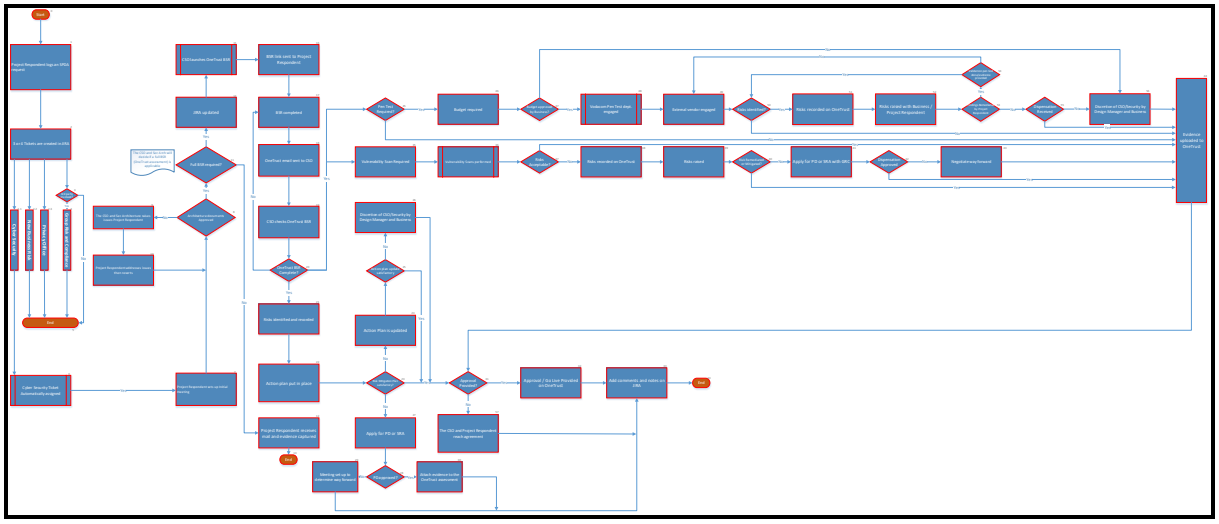


Figure 1- Cyber Security SPDA Process

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 competing 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

- 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

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

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:

SPDA Process.vsdx

SPDA Process.pdf

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

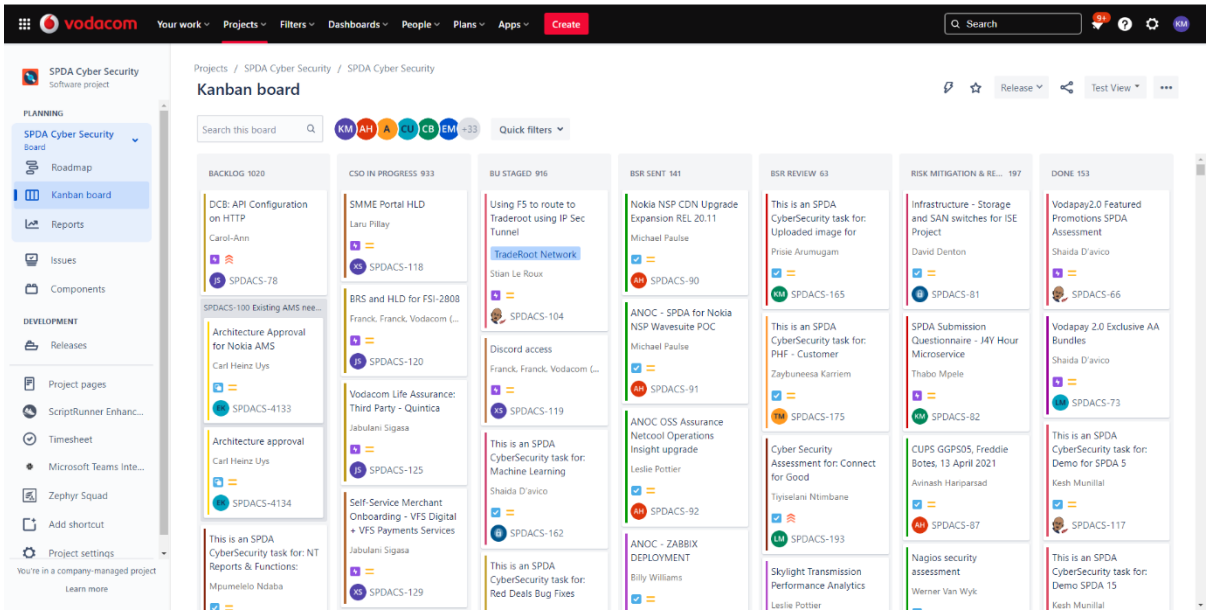


Figure 2

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

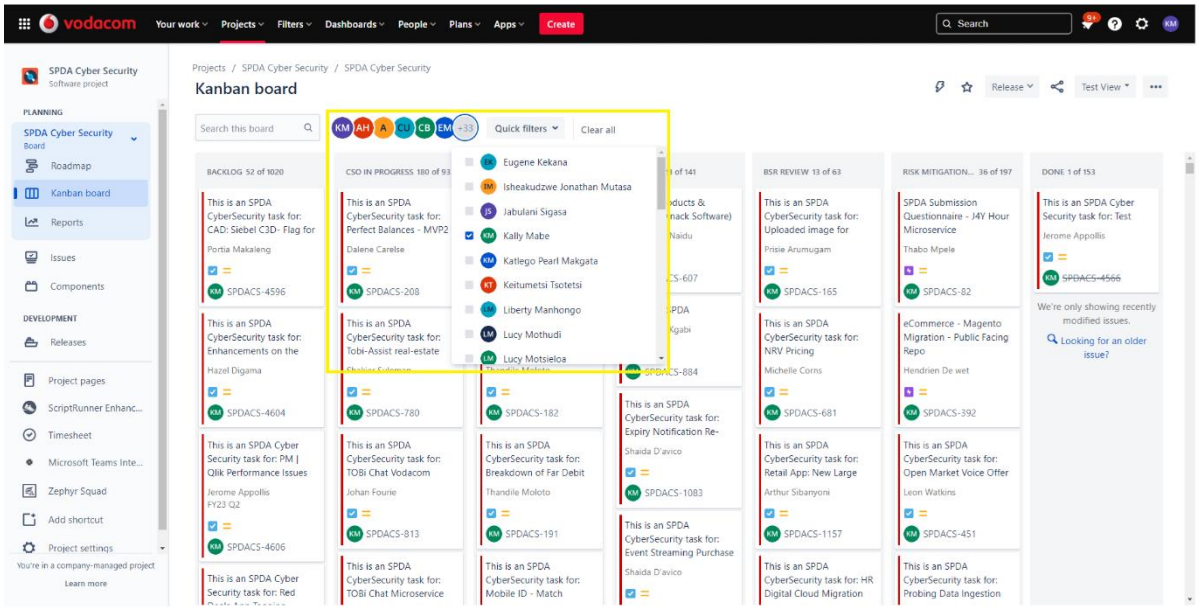


Figure 3

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

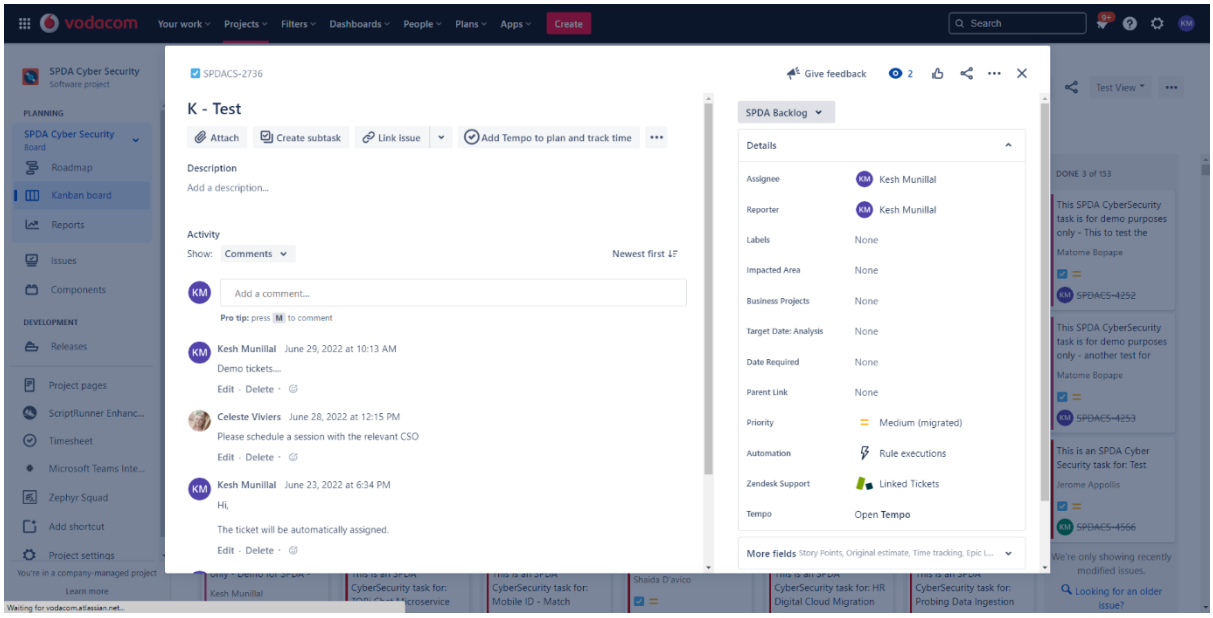


Figure 4

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

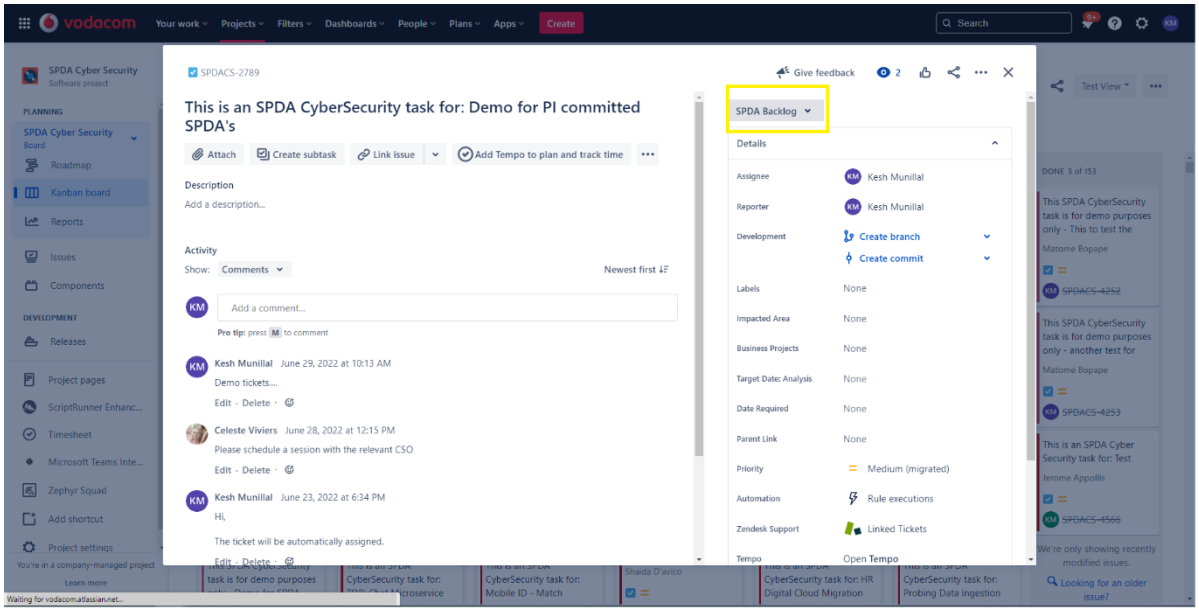


Figure 5

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,

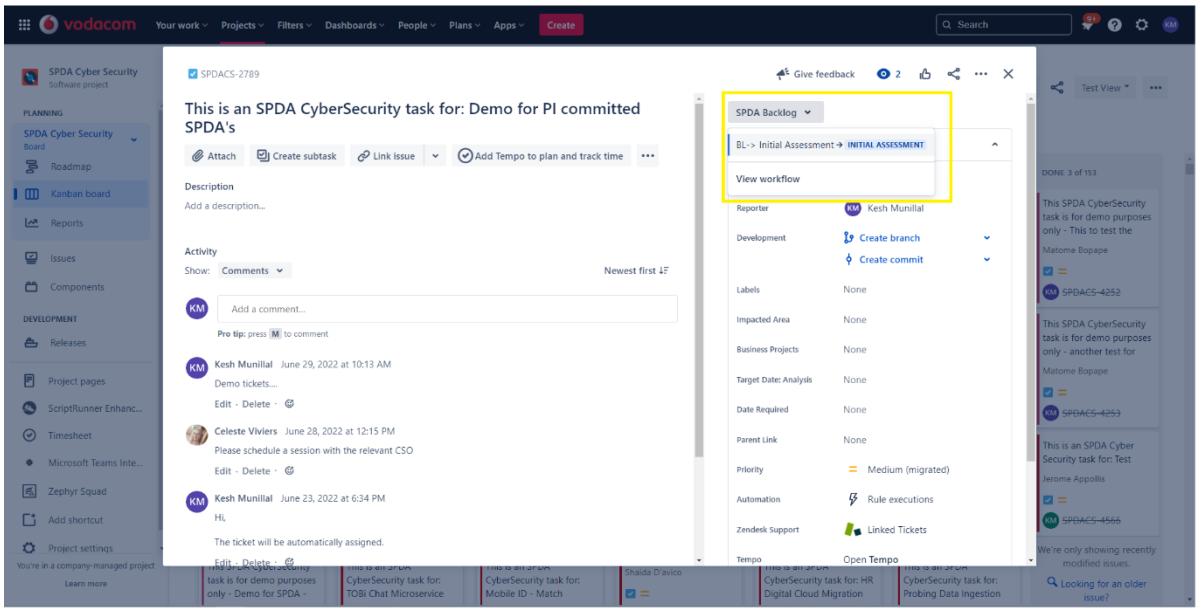


Figure 6

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

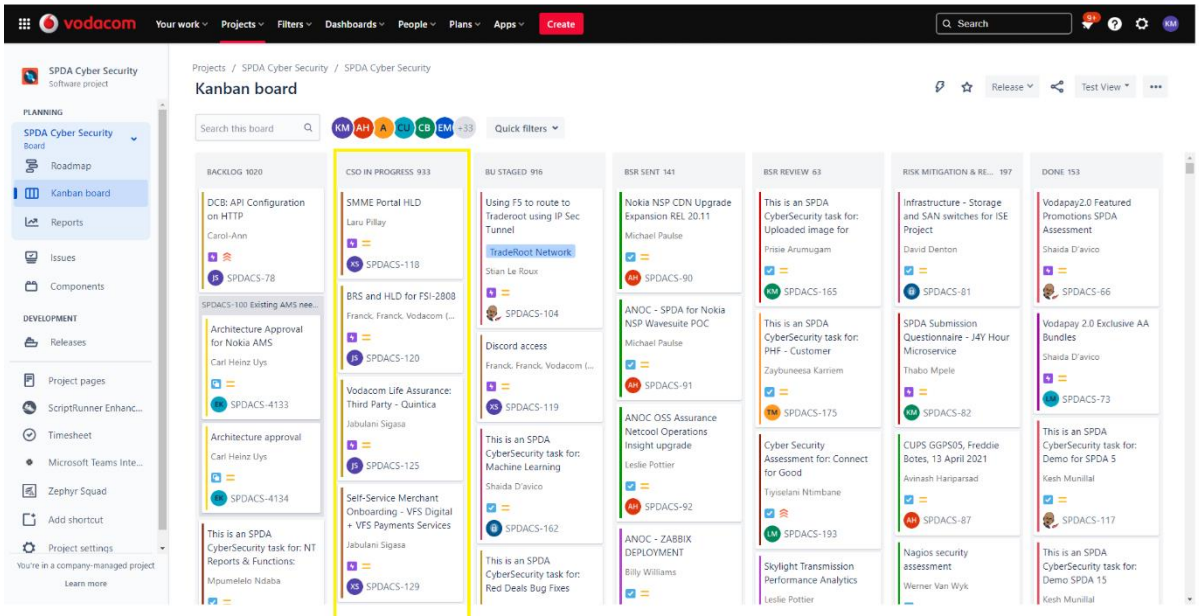


Figure 7

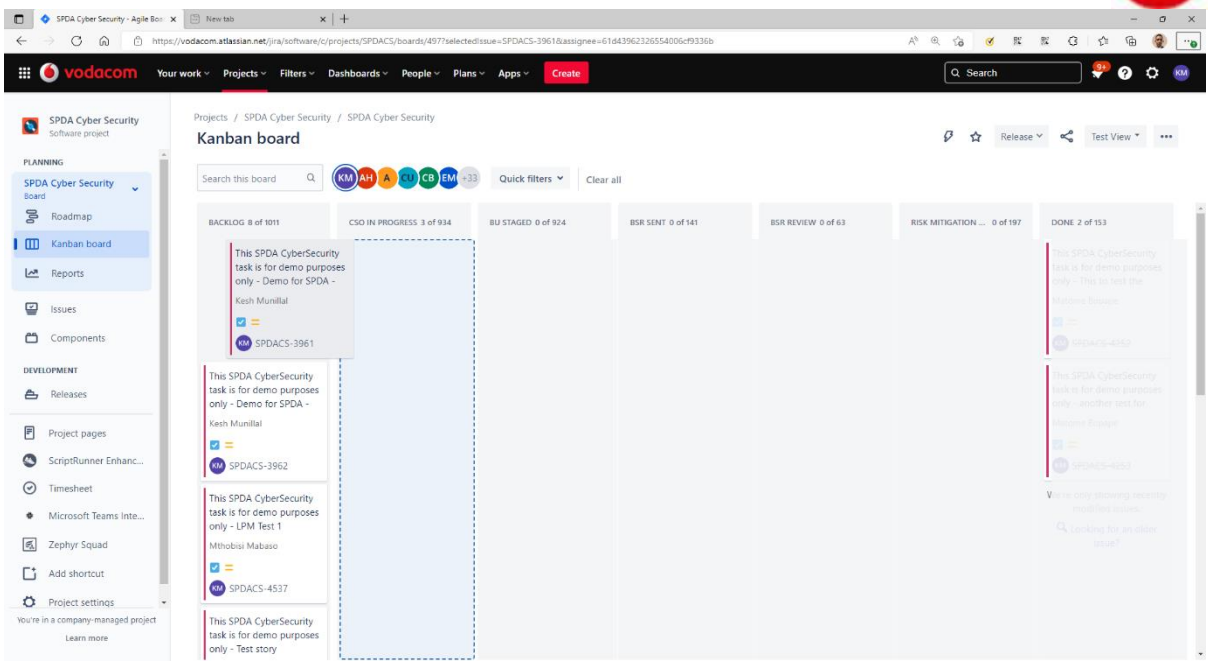


Figure 8

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

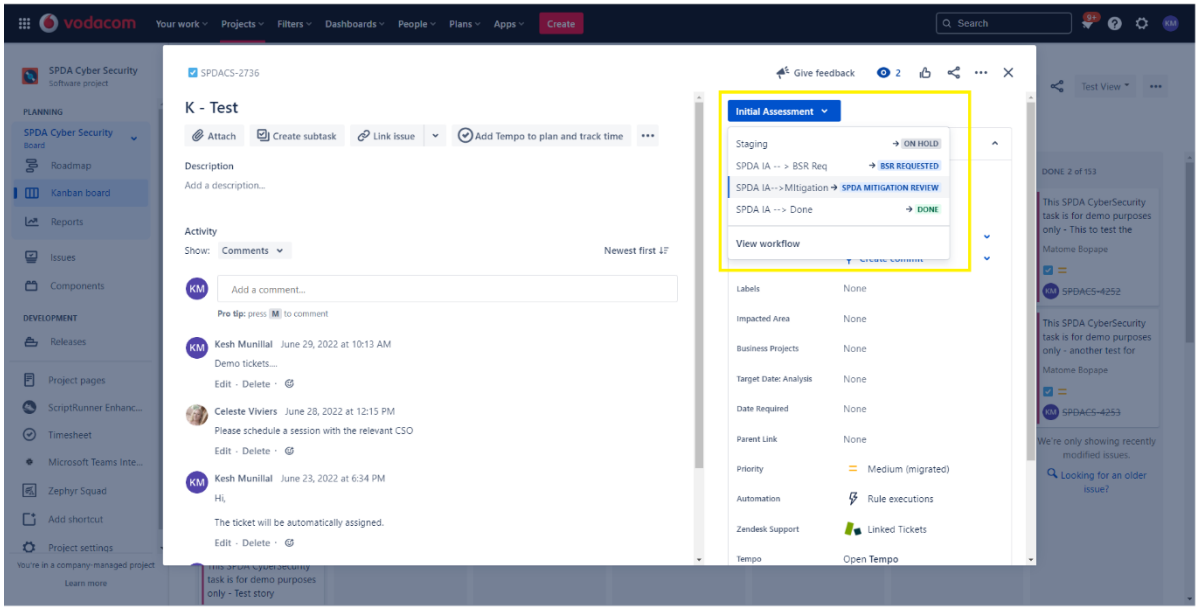


Figure 9

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

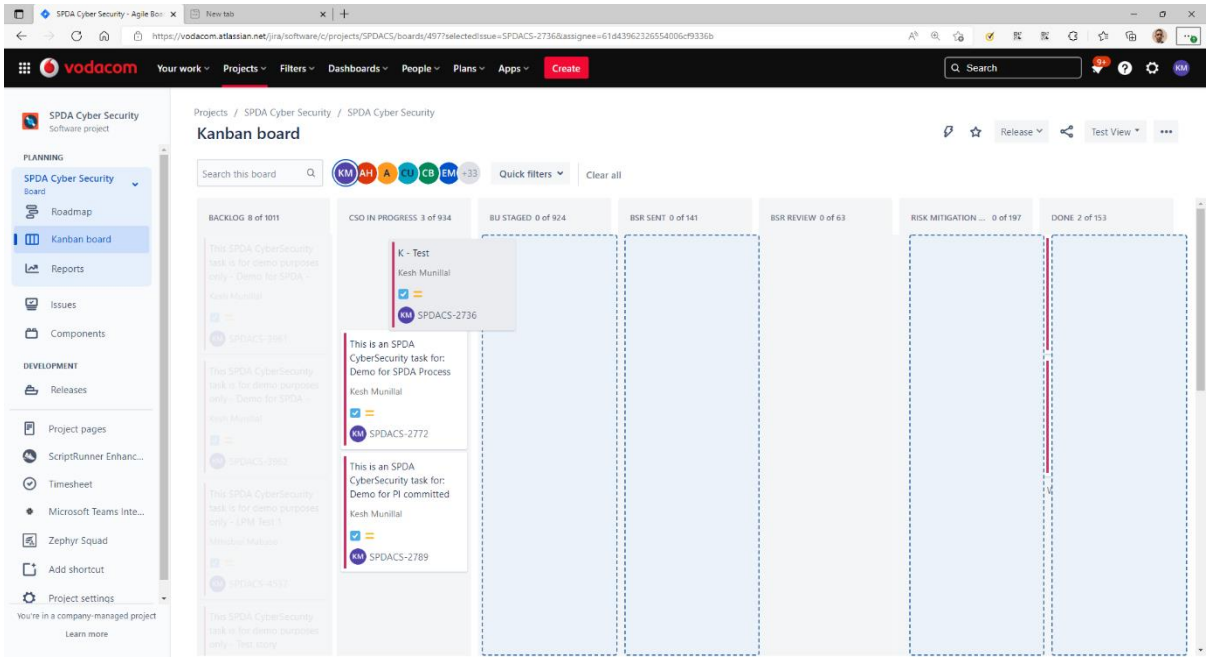


Figure 10

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'

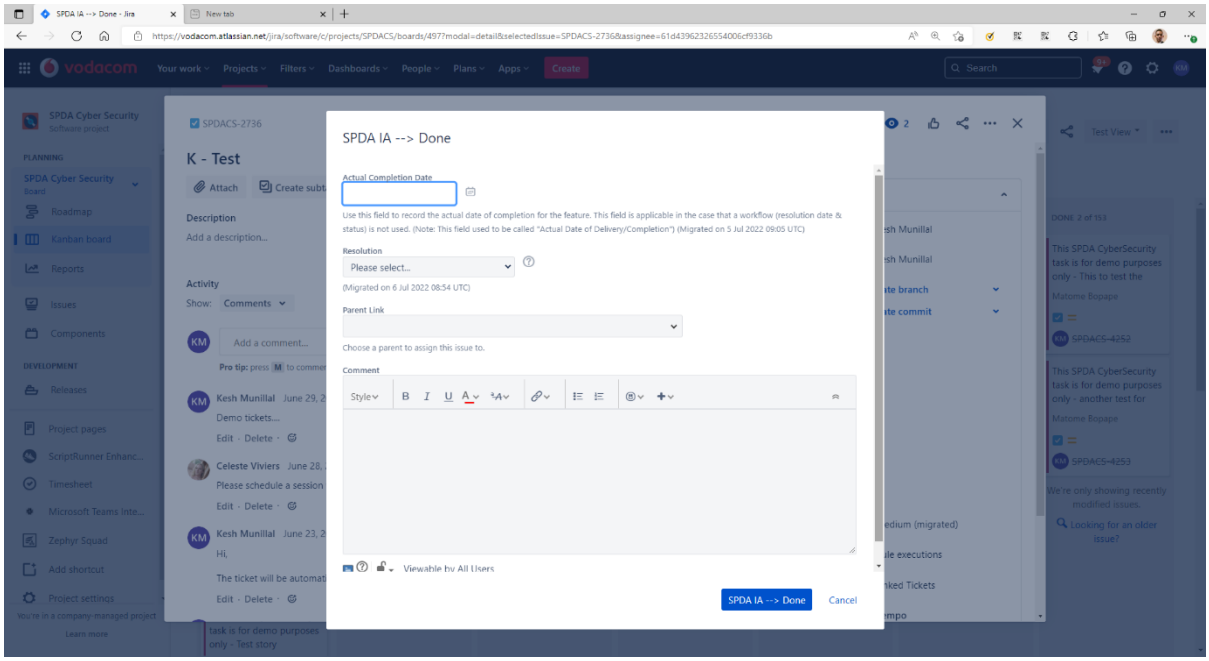
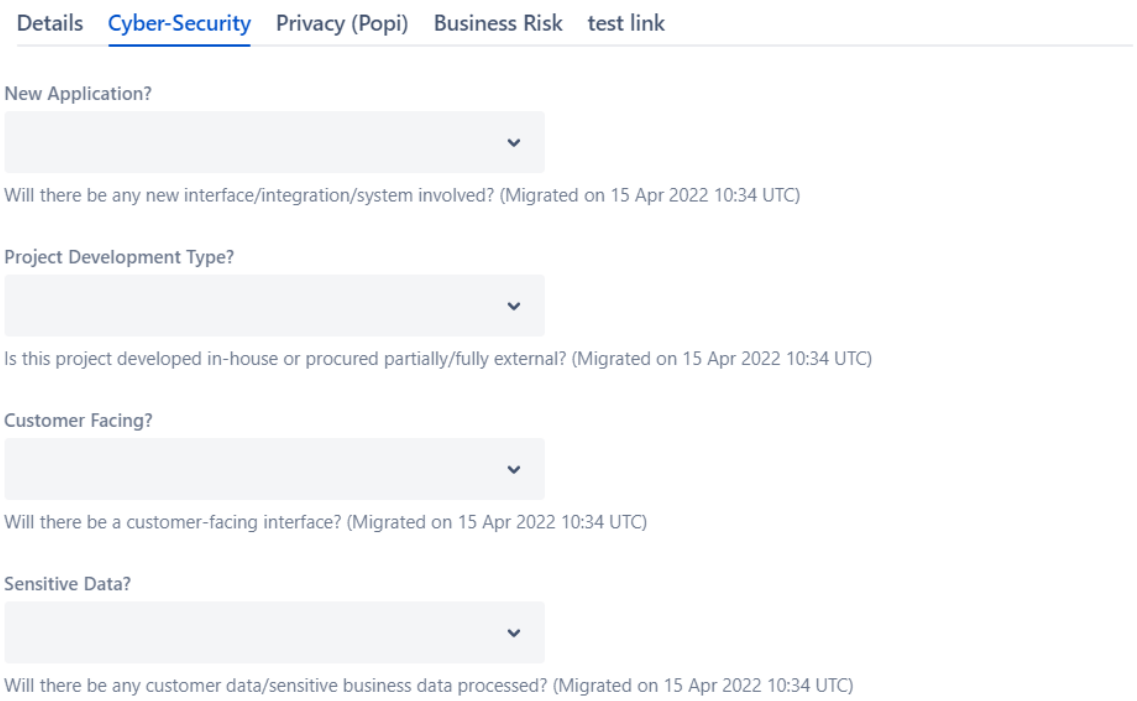


Figure 11

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:



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)

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)

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)

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
Plannned 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)	☐
Not Contained in an existing document	☐

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	Yes ☐	No ☐	Partial ☐	N/A ☐	
Are you using existing infrastructure to implement?	Yes ☐	No ☐	Partial ☐	N/A ☐	
Do you need a new environment?	Yes ☐	No ☐	Partial ☐	N/A ☐	
Is this a new commercial offering to customers?	Yes ☐	No ☐	Partial ☐	N/A ☐	
Is this an enhancement/addition to an existing commercial offering to customers?	Yes ☐	No ☐	Partial ☐	N/A ☐	
Product / service stays exactly the same - simply introducing a new supplier	Yes ☐	No ☐	Partial ☐	N/A ☐	

Business / Partnering model for this product / service					Additional Notes / Clarification
Is this a new business model	Yes ☐	No ☐	Partial ☐	N/A ☐	
VC Only product / service	Yes ☐	No ☐	Partial ☐	N/A ☐	
Partner ONLY : (VC Branded)	Yes ☐	No ☐	Partial ☐	N/A ☐	
Partner ONLY : (NOT VC Branded)	Yes ☐	No ☐	Partial ☐	N/A ☐	
Combined VC and Partner initiative (VC Branded)	Yes ☐	No ☐	Partial ☐	N/A ☐	
Combined VC and Partner initiative (NOT VC Branded)	Yes ☐	No ☐	Partial ☐	N/A ☐	

Please tick all of the following Technical detail that applies:

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

Technical Hosting Information:

Which of the following is your application hosted on?	Cloud ☐	On Prem ☐	Third Party ☐

If Third Party is ticked, please provide:

Third Party Information Required	Answer:				Please Elaborate
When was the last third party assessment done	Yes ☐	No ☐	Partial ☐	N/A ☐	*Provide date*
Any existing Audit, risks, or vulnerabilities that affect the application directly or indirectly	Yes ☐	No ☐	Partial ☐	N/A ☐	*Attach the risk register*
Is the third party assessment still valid?	Yes ☐	No ☐	Partial ☐	N/A ☐	*Attach the evidence here*
Is there a new partner / vendor / supplier involved with this product / service?	Yes ☐	No ☐	Partial ☐	N/A ☐	
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 ☐	No ☐	Partial ☐	N/A ☐	
Authentication Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Financial Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Customer Care Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Content Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Call, Internet and/or Television Traffic Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Location Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Data about Device	Yes ☐	No ☐	Partial ☐	N/A ☐	
Data from Device	Yes ☐	No ☐	Partial ☐	N/A ☐	
Profiling Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Public Identity Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Special categories of Personal Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Biometric identifiers or similar physical-based data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Other:					
Employee Data Types					
Recruitment Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Sensitive Employee Personal Data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Employment Details	Yes ☐	No ☐	Partial ☐	N/A ☐	
Salary and Payment Details	Yes ☐	No ☐	Partial ☐	N/A ☐	
Performance Details	Yes ☐	No ☐	Partial ☐	N/A ☐	
HR Administration and Support	Yes ☐	No ☐	Partial ☐	N/A ☐	
Employee Authentication or log in Details	Yes ☐	No ☐	Partial ☐	N/A ☐	
Employee Wellbeing details	Yes ☐	No ☐	Partial ☐	N/A ☐	
Health and Safety Records	Yes ☐	No ☐	Partial ☐	N/A ☐	
Biometric and similar physical based details	Yes ☐	No ☐	Partial ☐	N/A ☐	
Content of Employee Communications	Yes ☐	No ☐	Partial ☐	N/A ☐	
Device Based or related data for corporate devices	Yes ☐	No ☐	Partial ☐	N/A ☐	
Monitoring of Employees	Yes ☐	No ☐	Partial ☐	N/A ☐	
Other:					
Supplier Related Personal Data:					
Supplier's Employee data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Contract details	Yes ☐	No ☐	Partial ☐	N/A ☐	
Electronic Signature	Yes ☐	No ☐	Partial ☐	N/A ☐	
Biometric Signature	Yes ☐	No ☐	Partial ☐	N/A ☐	
Monitoring of Supplier's Employees	Yes ☐	No ☐	Partial ☐	N/A ☐	
Other:					
Visitor Related Personal Data					
Visitor details	Yes ☐	No ☐	Partial ☐	N/A ☐	
Biometric identifiers and similar physical-based data	Yes ☐	No ☐	Partial ☐	N/A ☐	
Other					

Initial Qualifying Questionnaire.xlsx

4. OneTrust: Launch SPDA Assessment BSR

Login Screen:

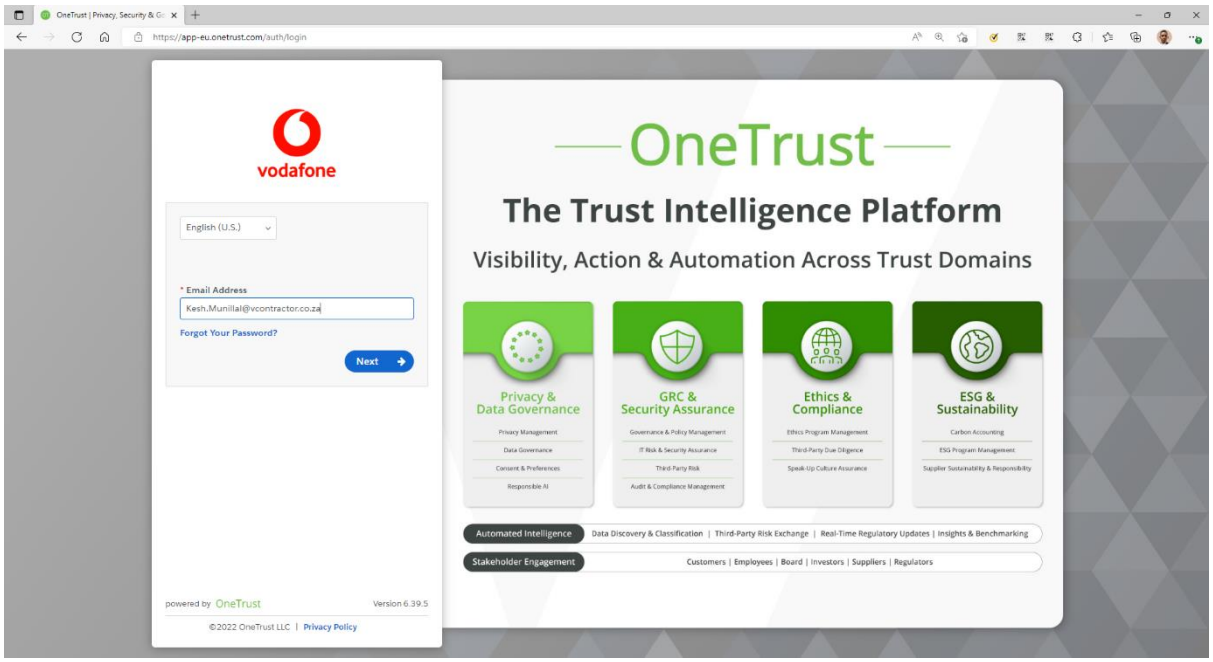


Figure 12

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

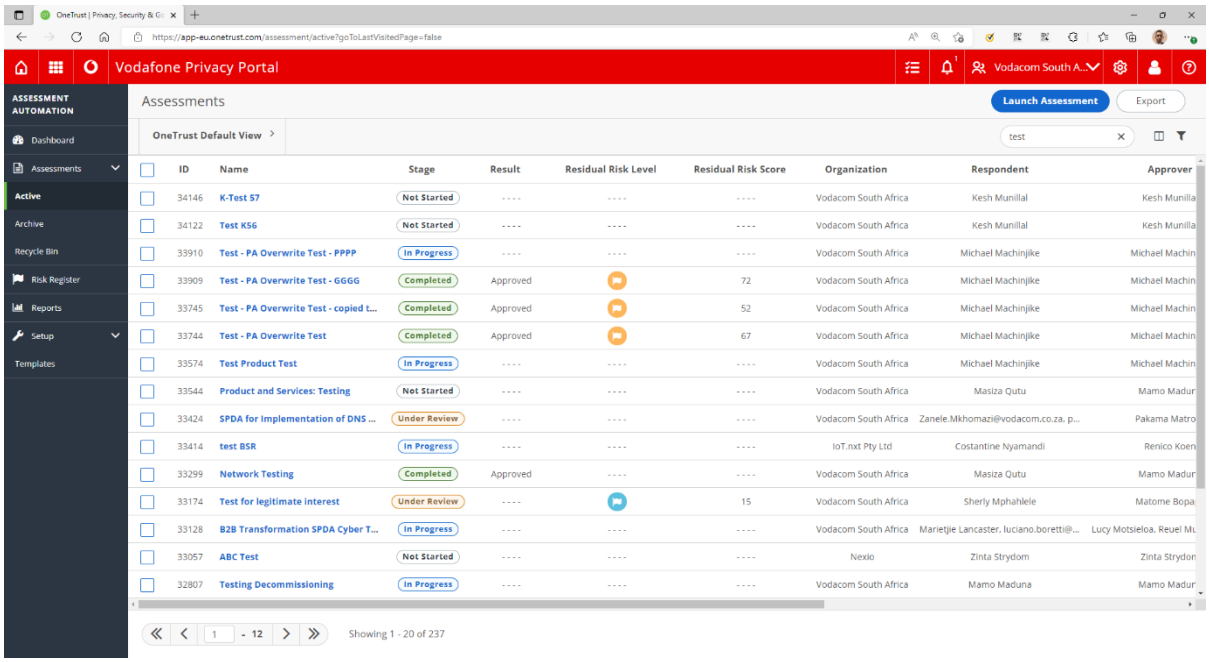


Figure 13

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

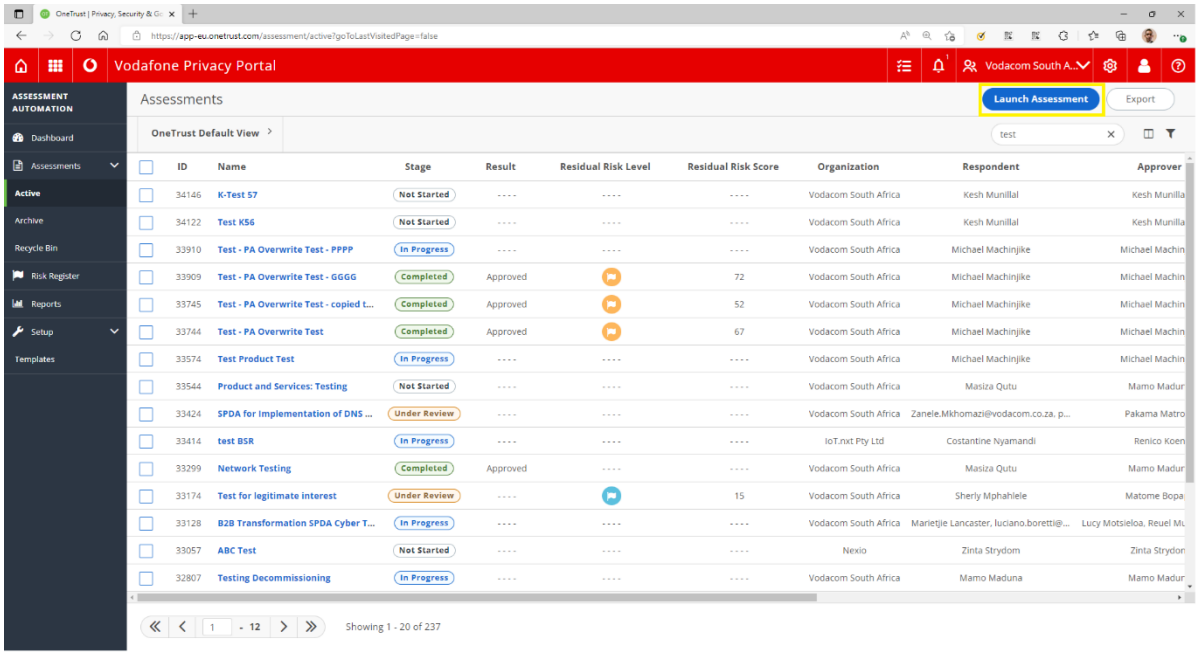


Figure 14

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

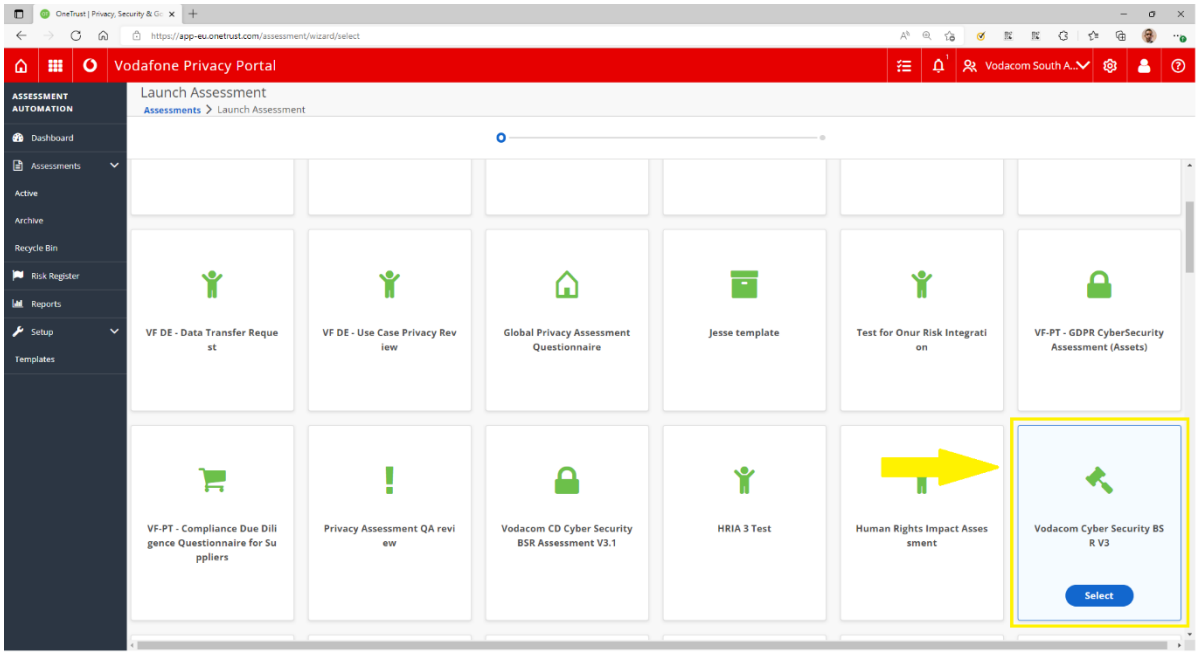


Figure 15

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

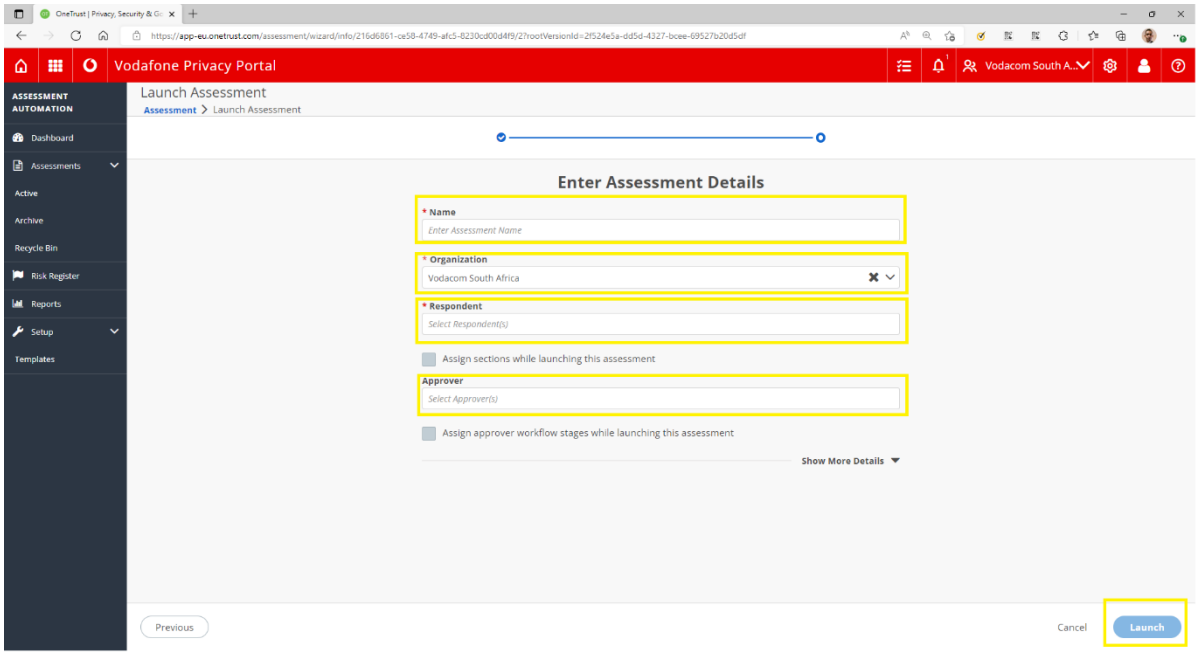


Figure 16

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

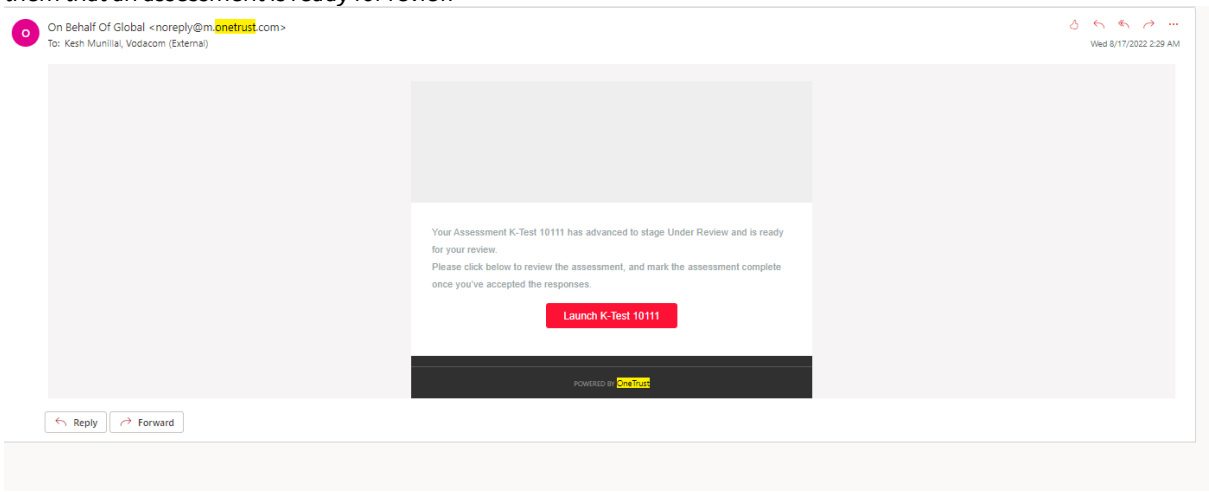


Figure 17

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

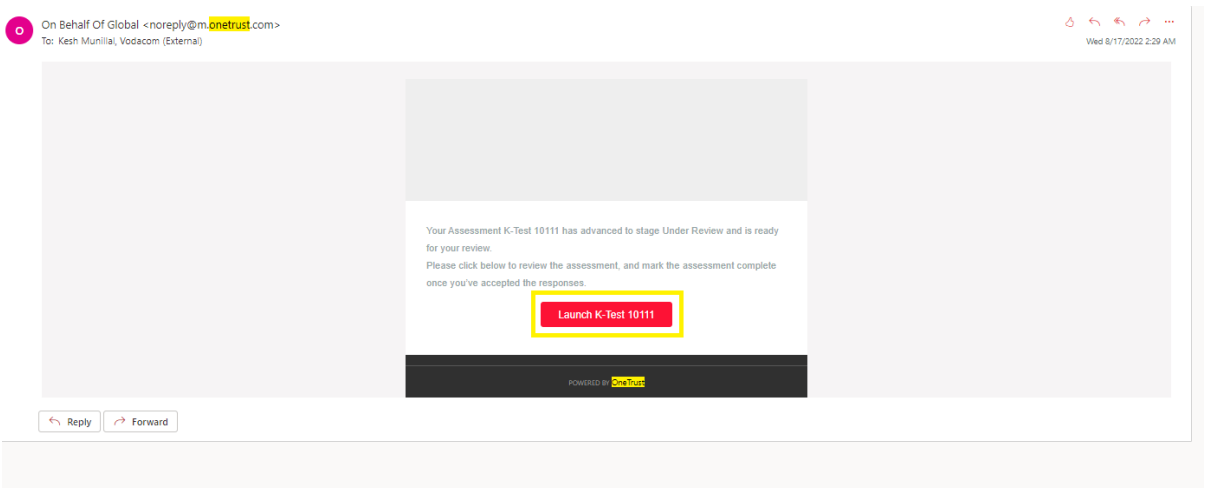


Figure 18

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

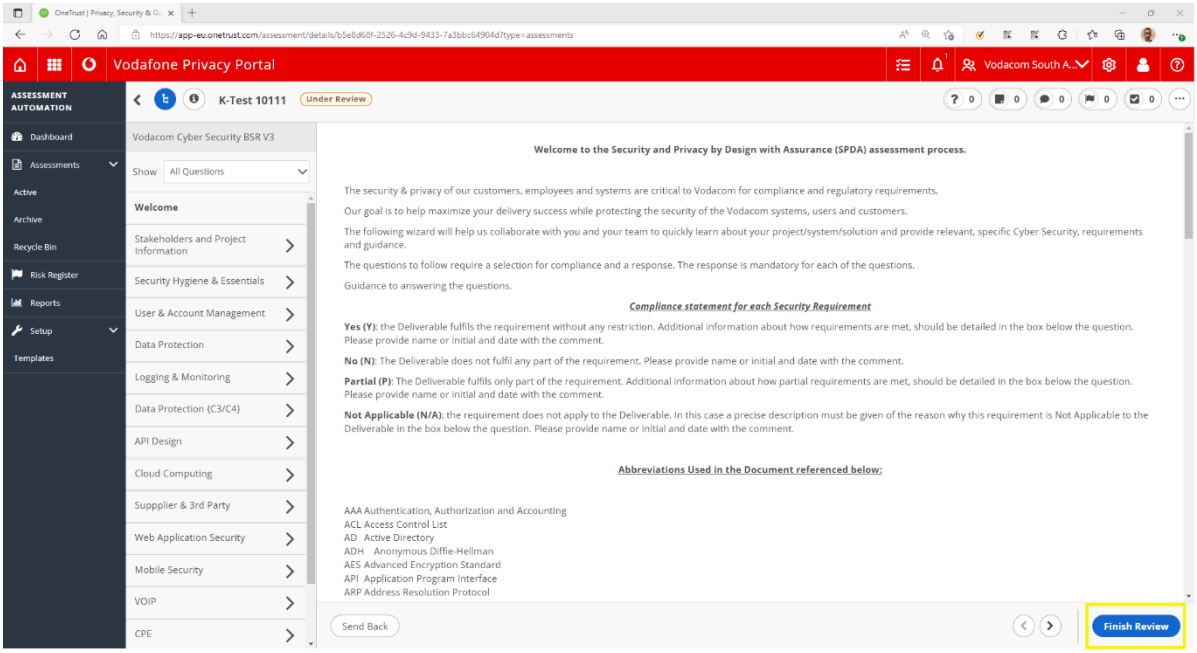


Figure 19

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

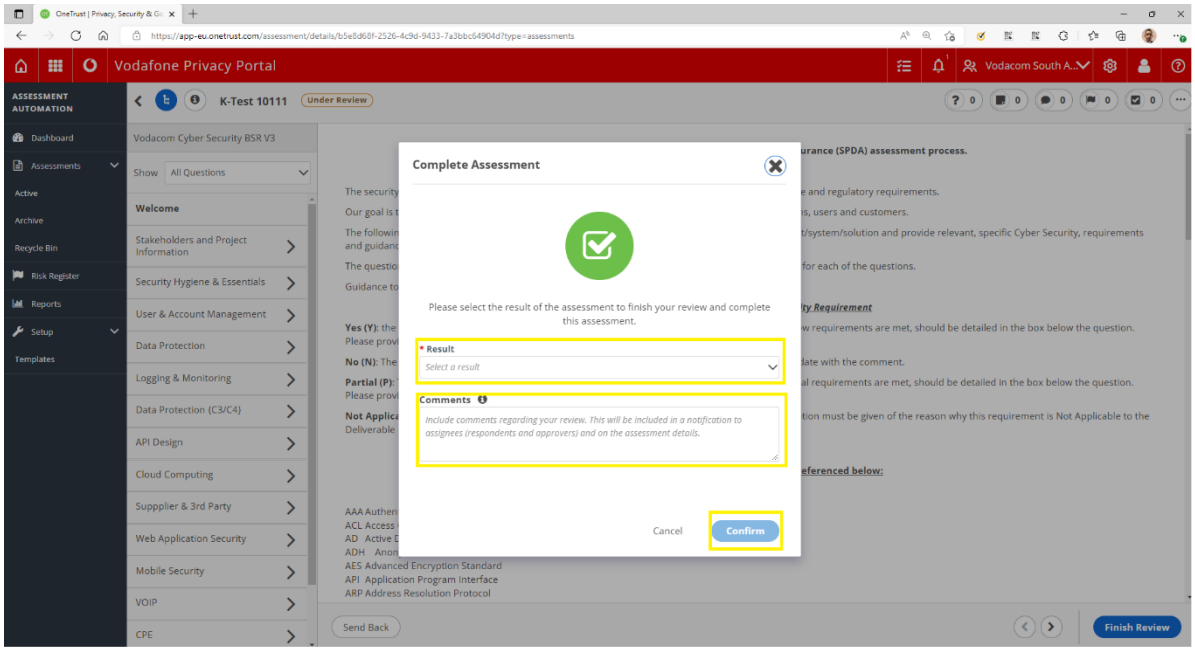


Figure 20

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

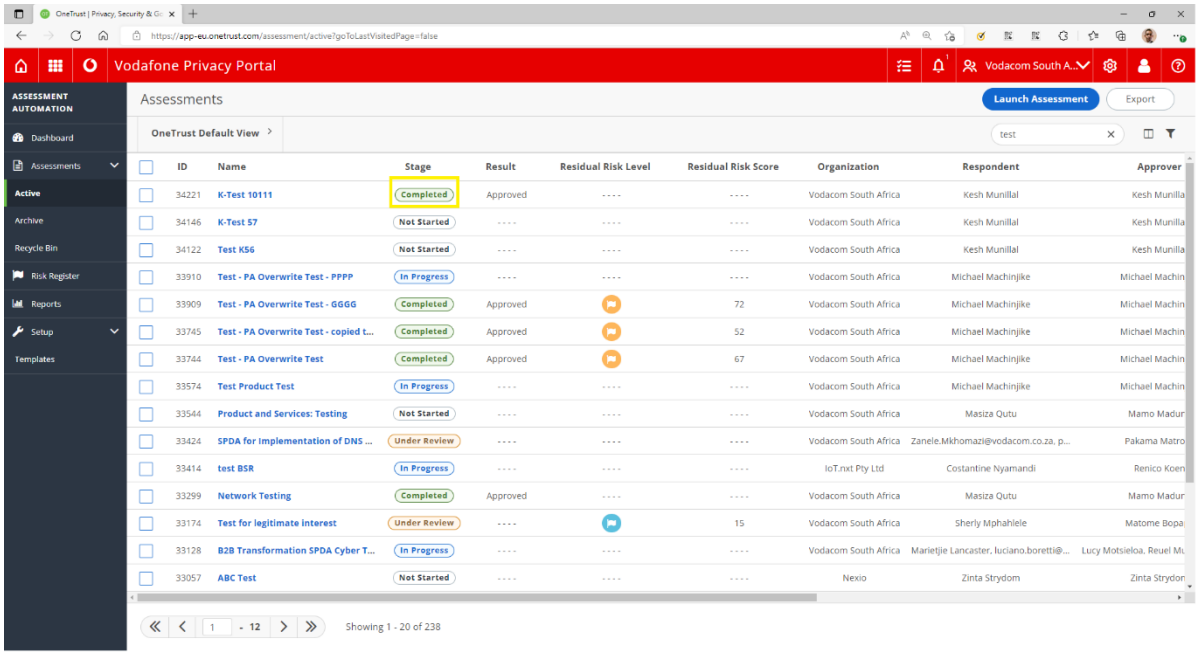


Figure 21

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

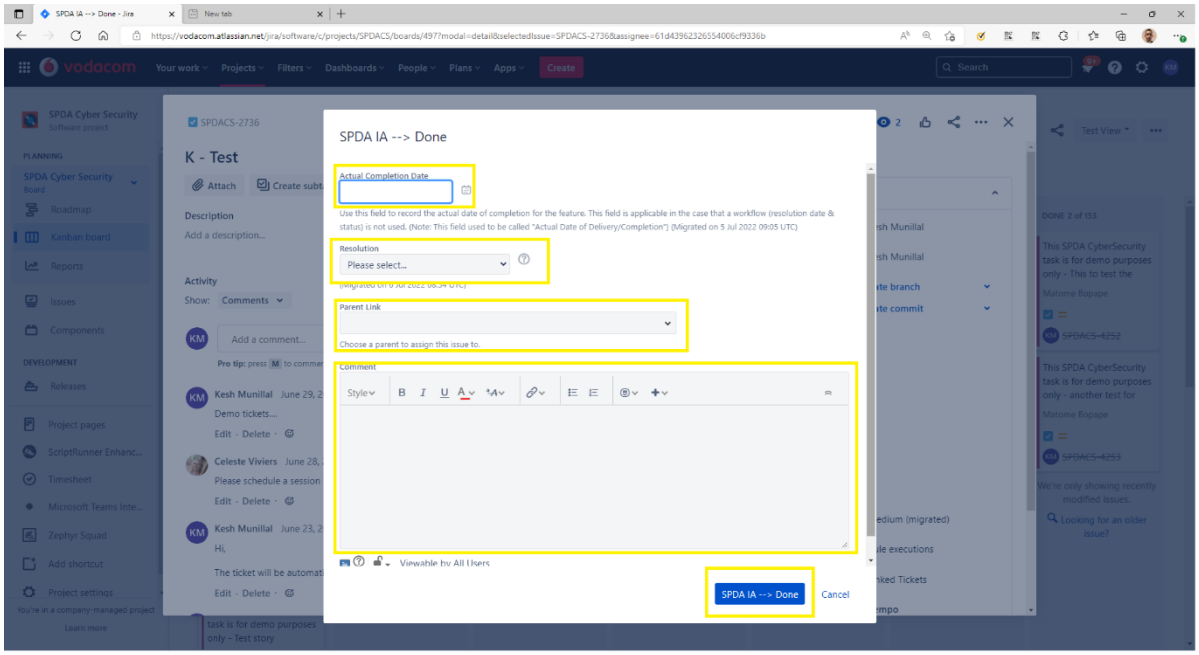


Figure 22

5. OneTrust: Cyber Security Assessment – Baseline Security Requirement

Welcome

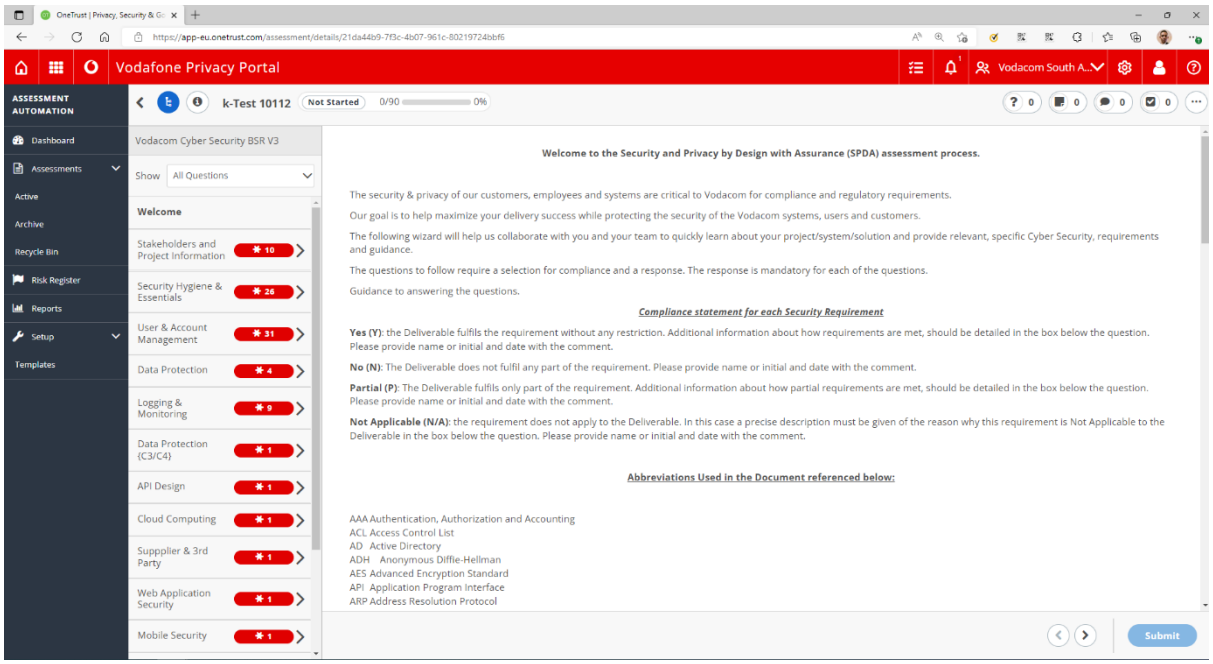


Figure 23

5.1 Select Stakeholder and Project Info

Questions 1.1 to 1.10

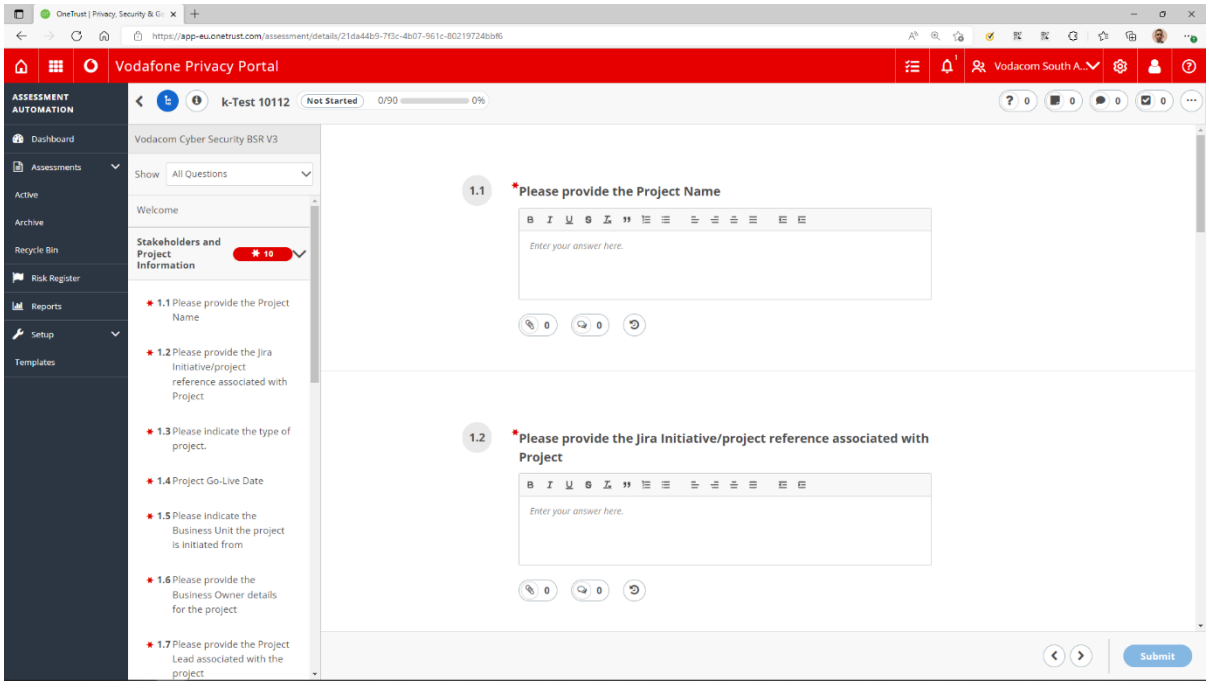


Figure 24

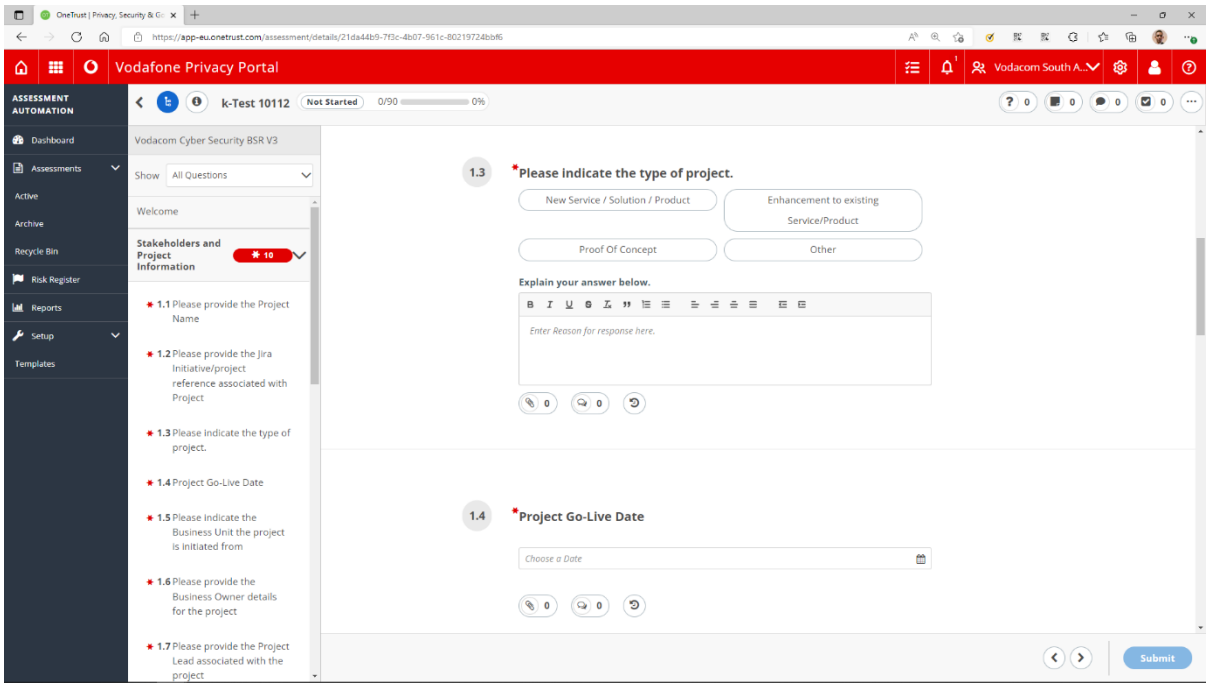


Figure 25

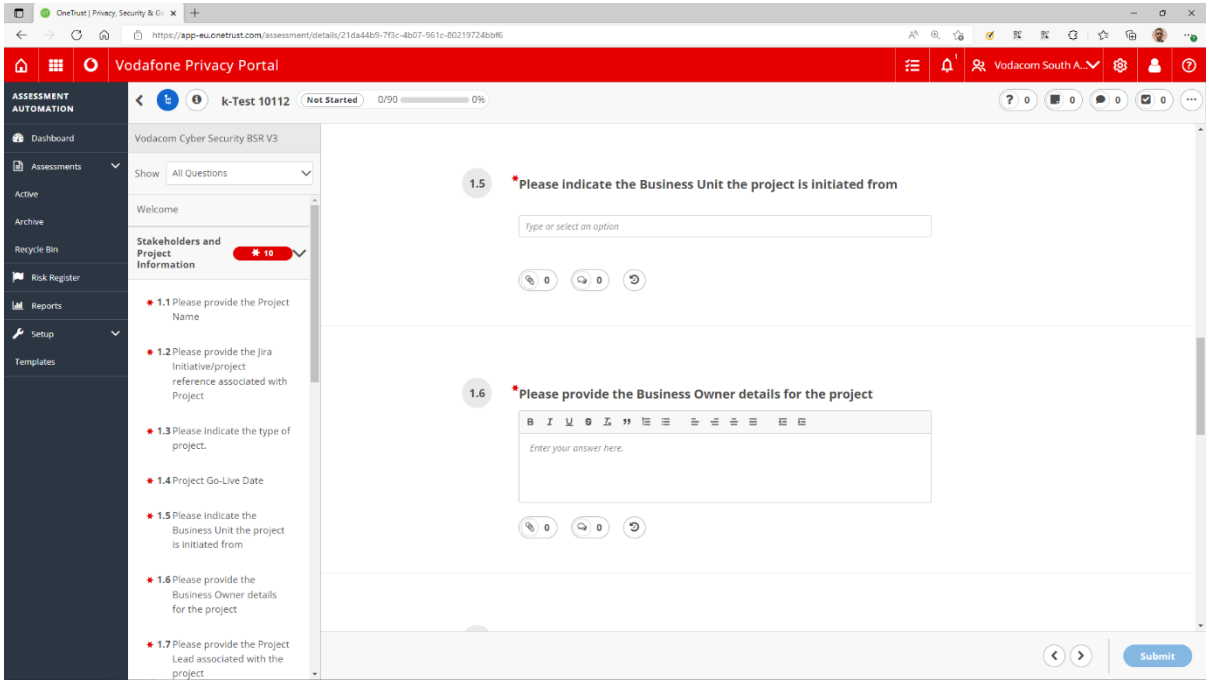


Figure 26

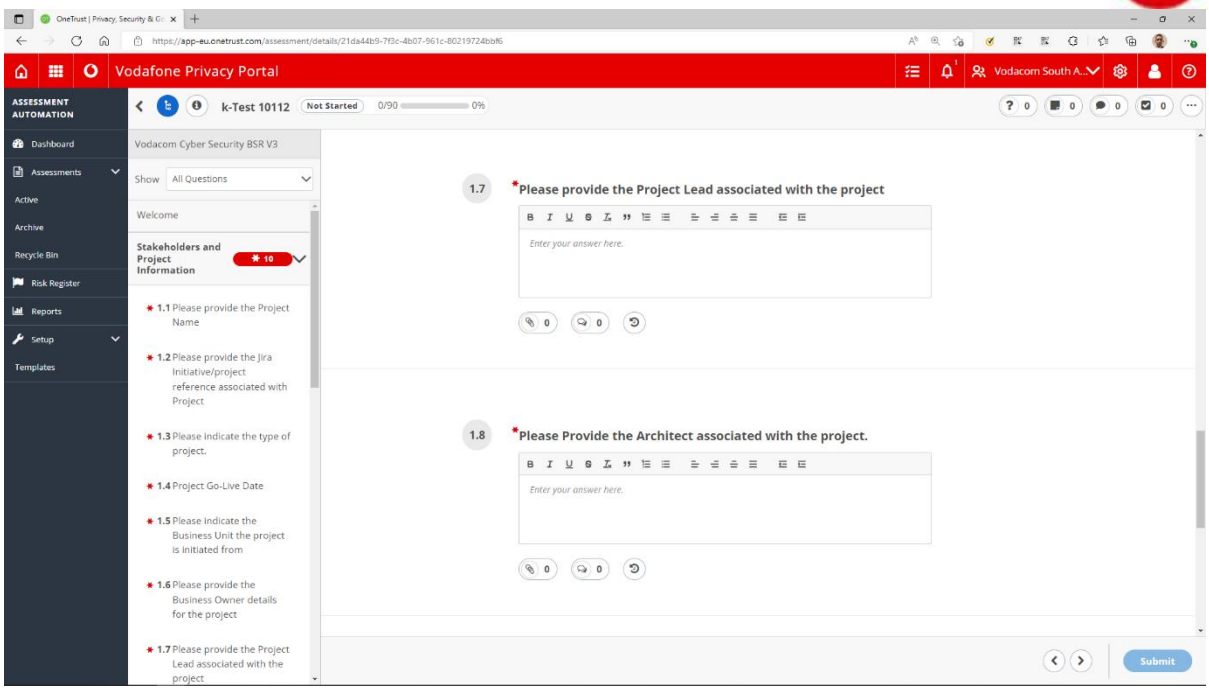


Figure 27

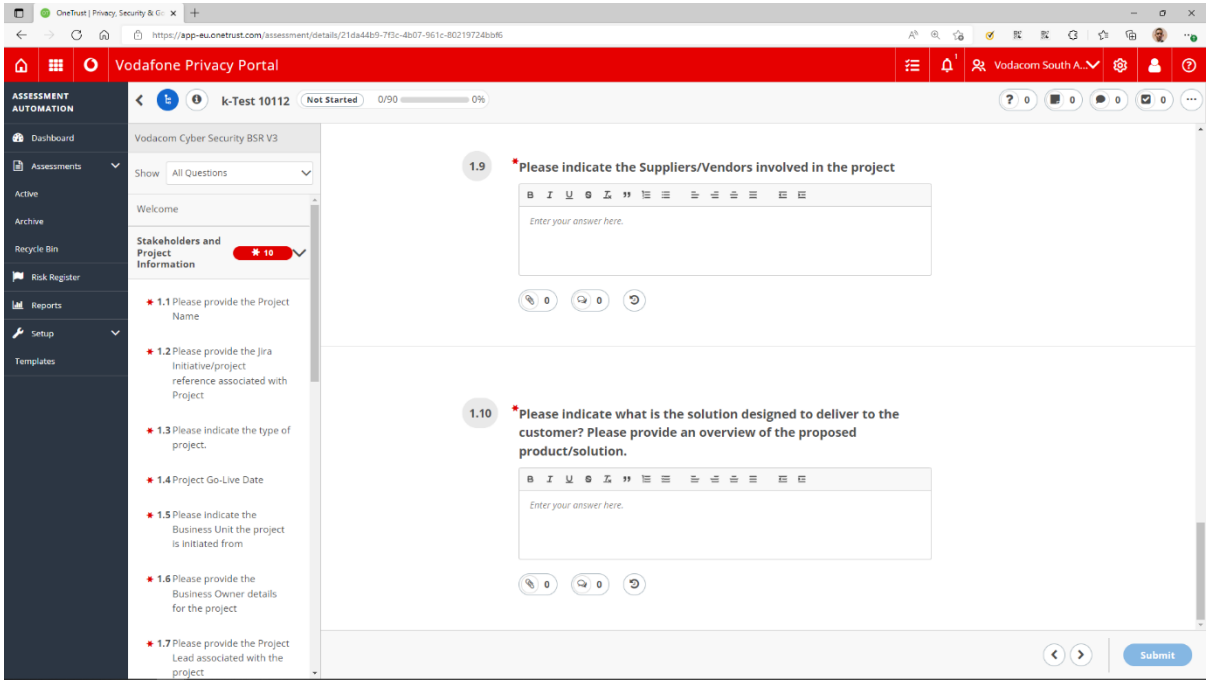


Figure 28

5.2 Security Hygiene and Essentials

Questions 2.1 to 2.35

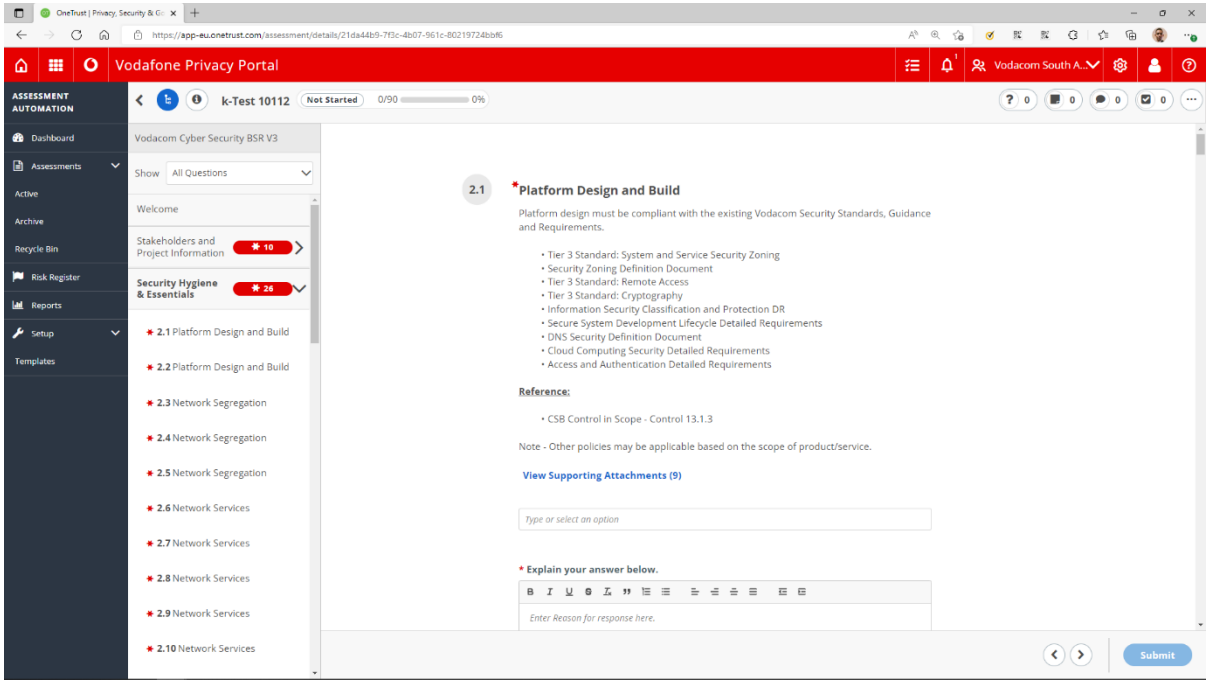


Figure 29

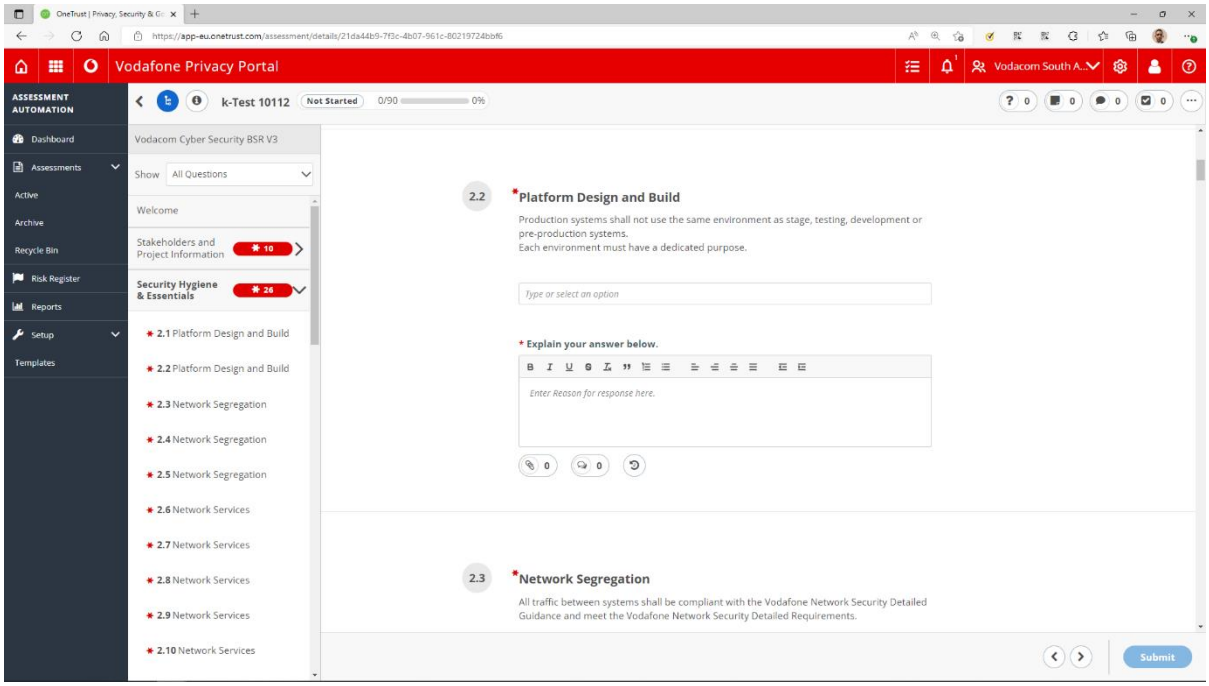


Figure 30

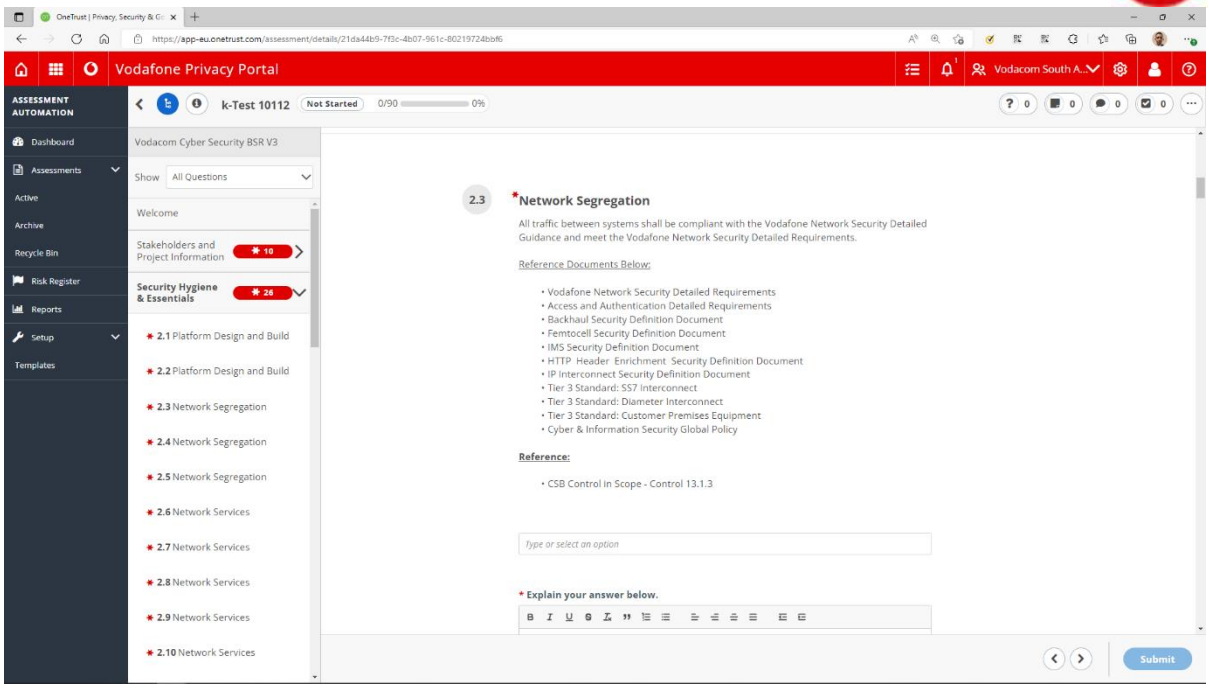


Figure 31

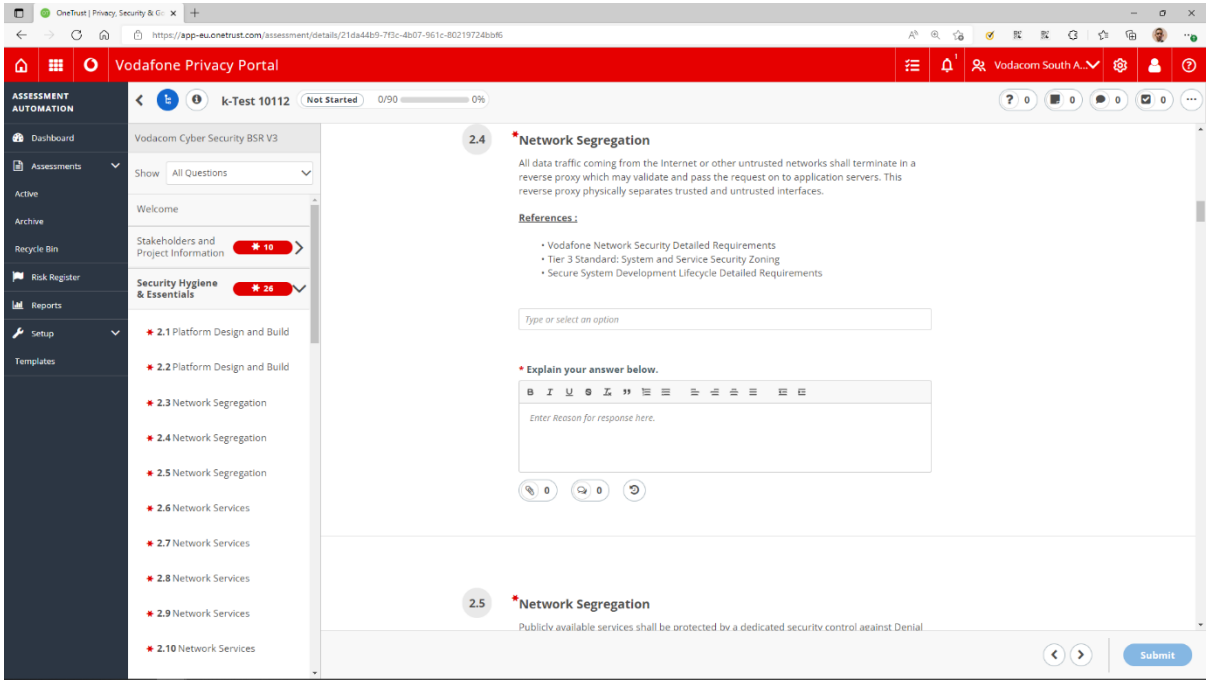


Figure 32

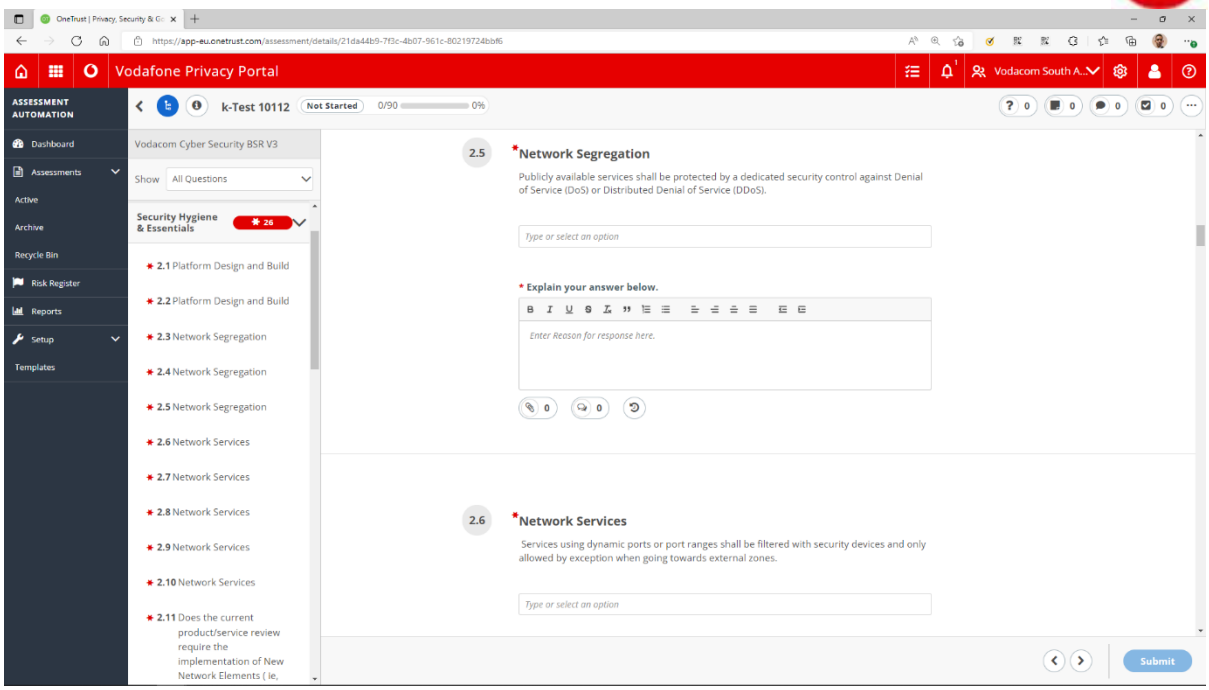


Figure 33

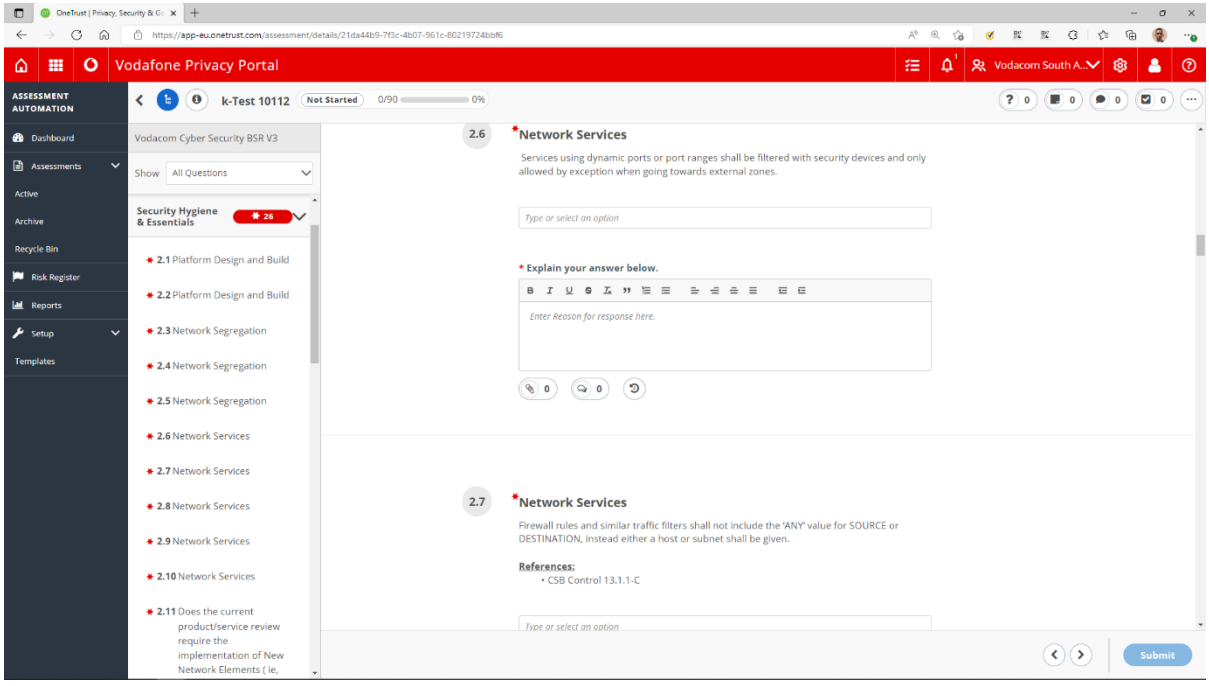


Figure 35

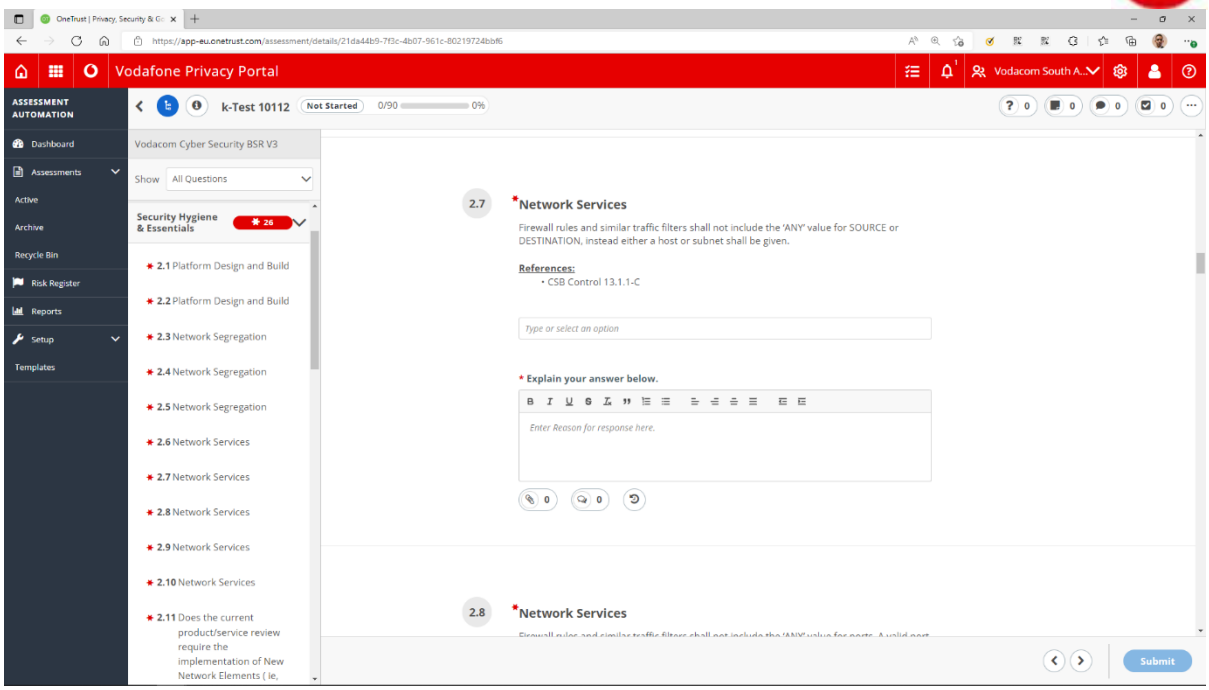


Figure 36

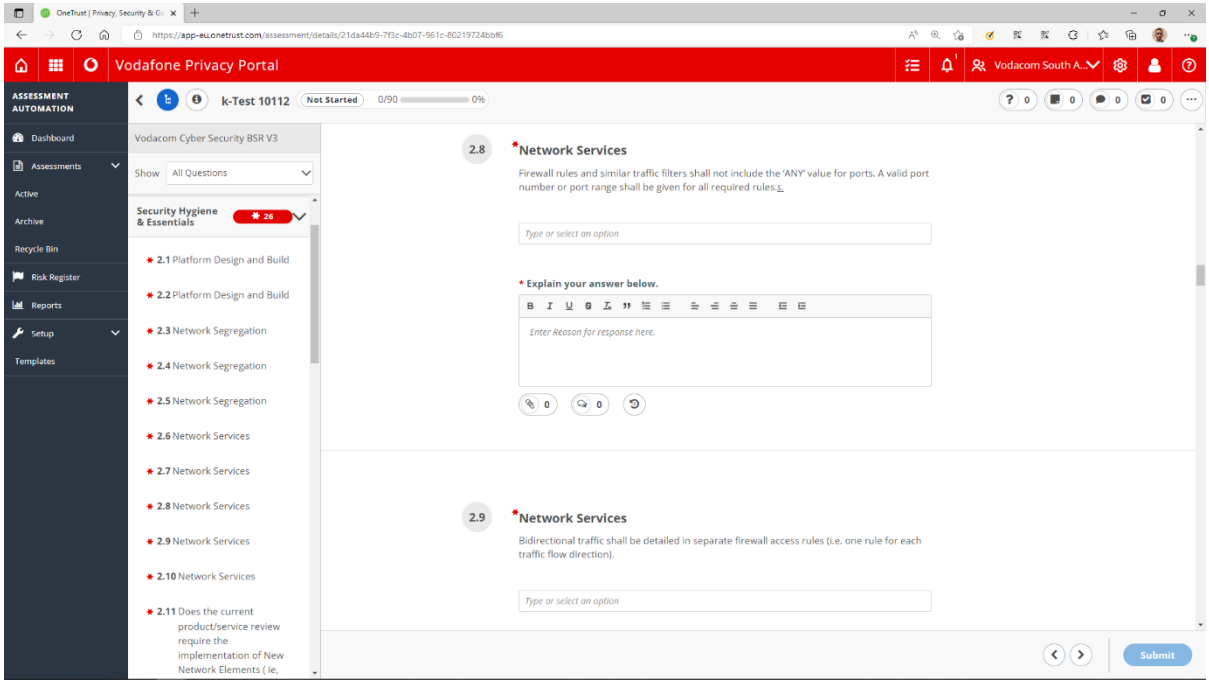


Figure 37

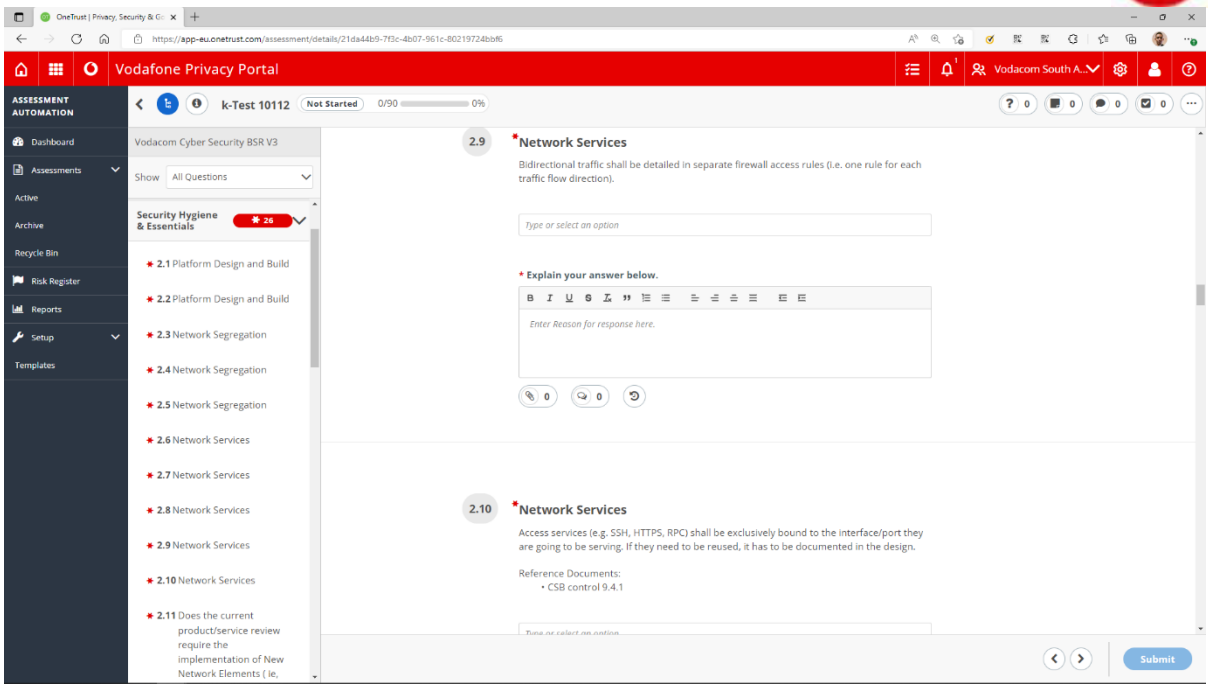


Figure 38

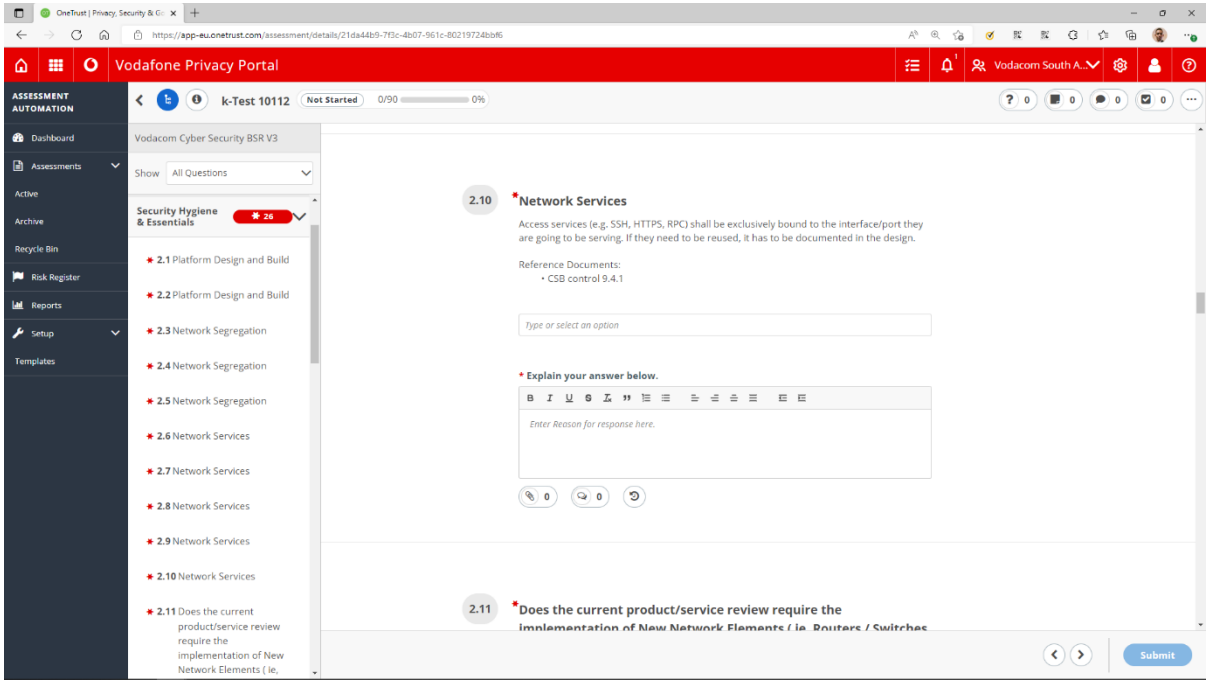


Figure 39

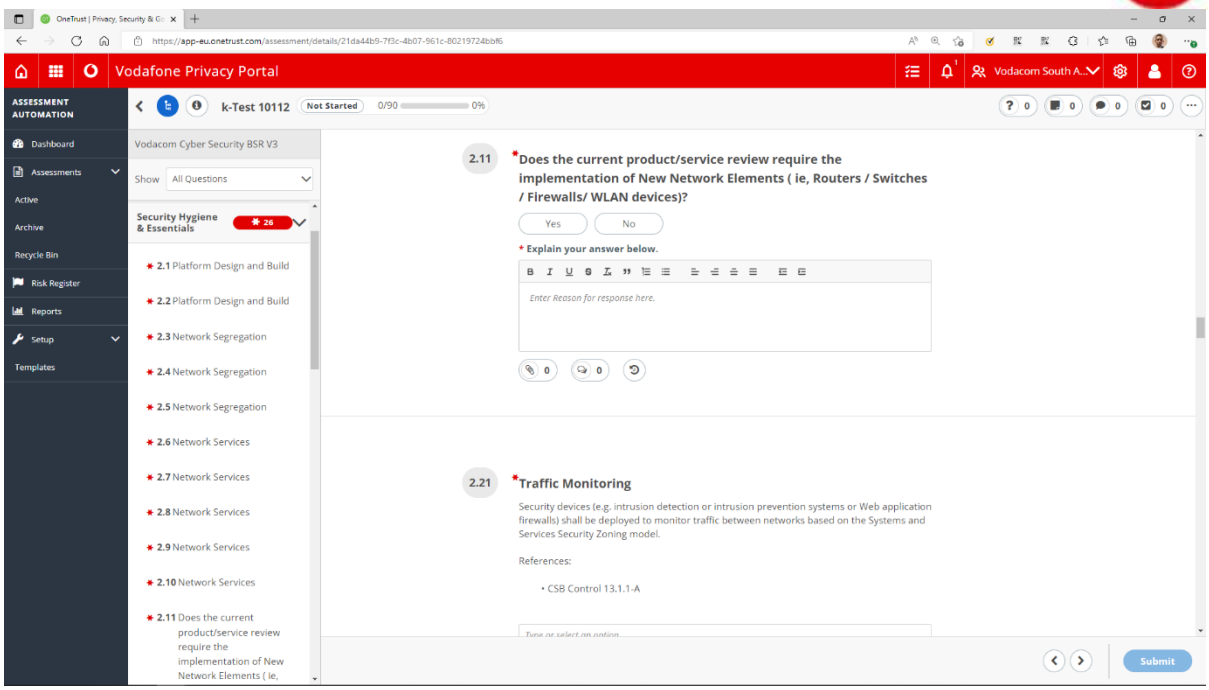


Figure 40

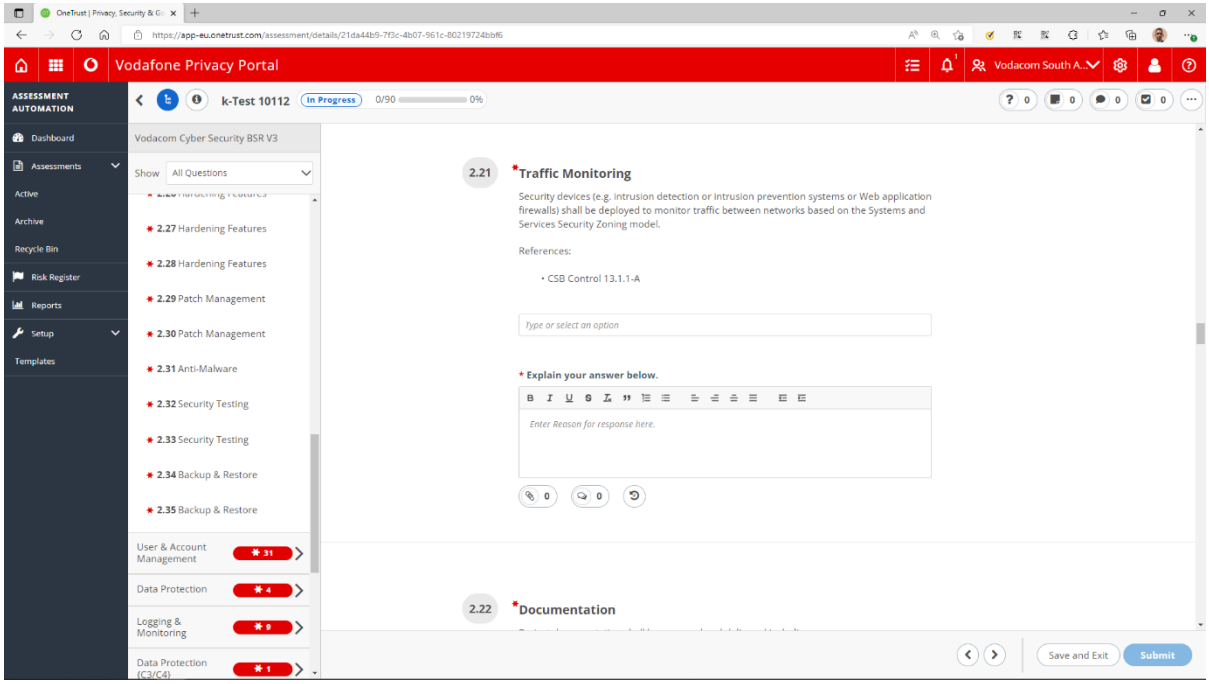


Figure 41

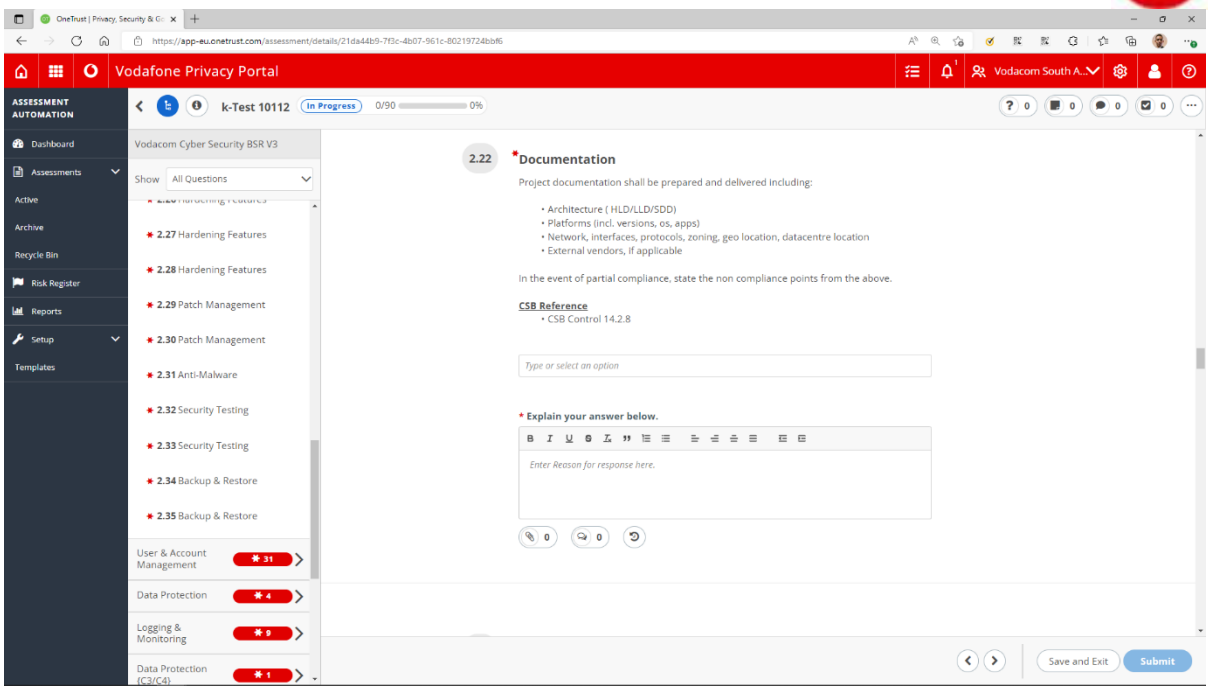


Figure 42

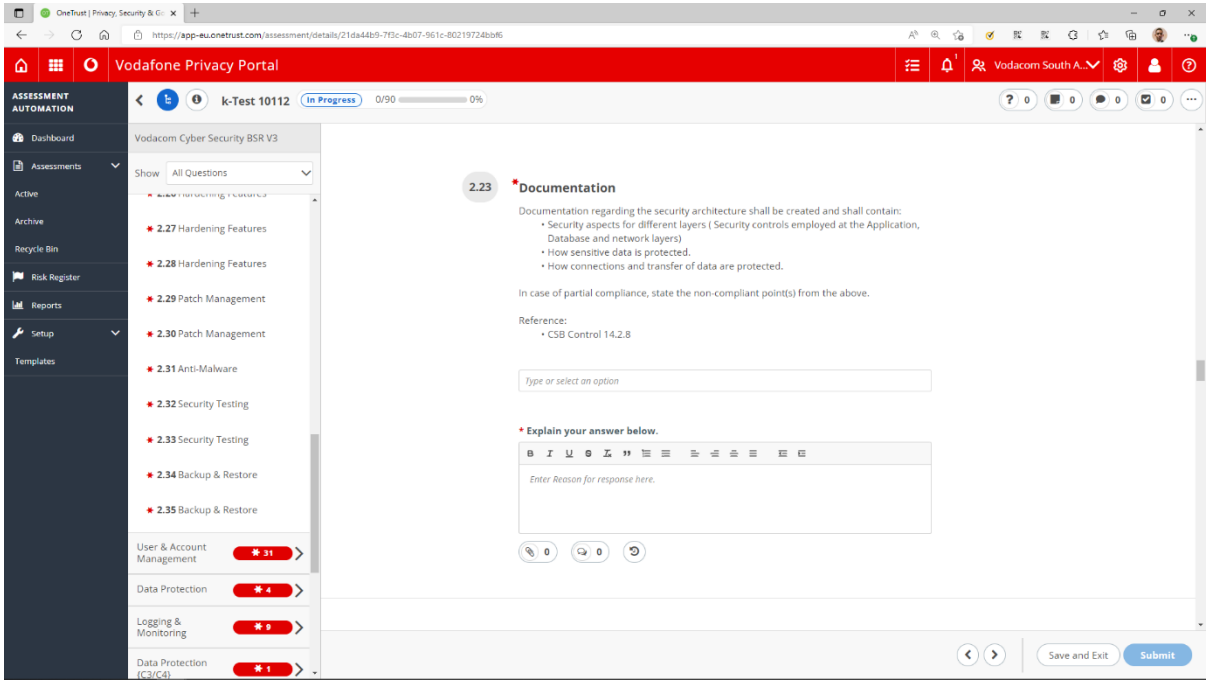


Figure 43

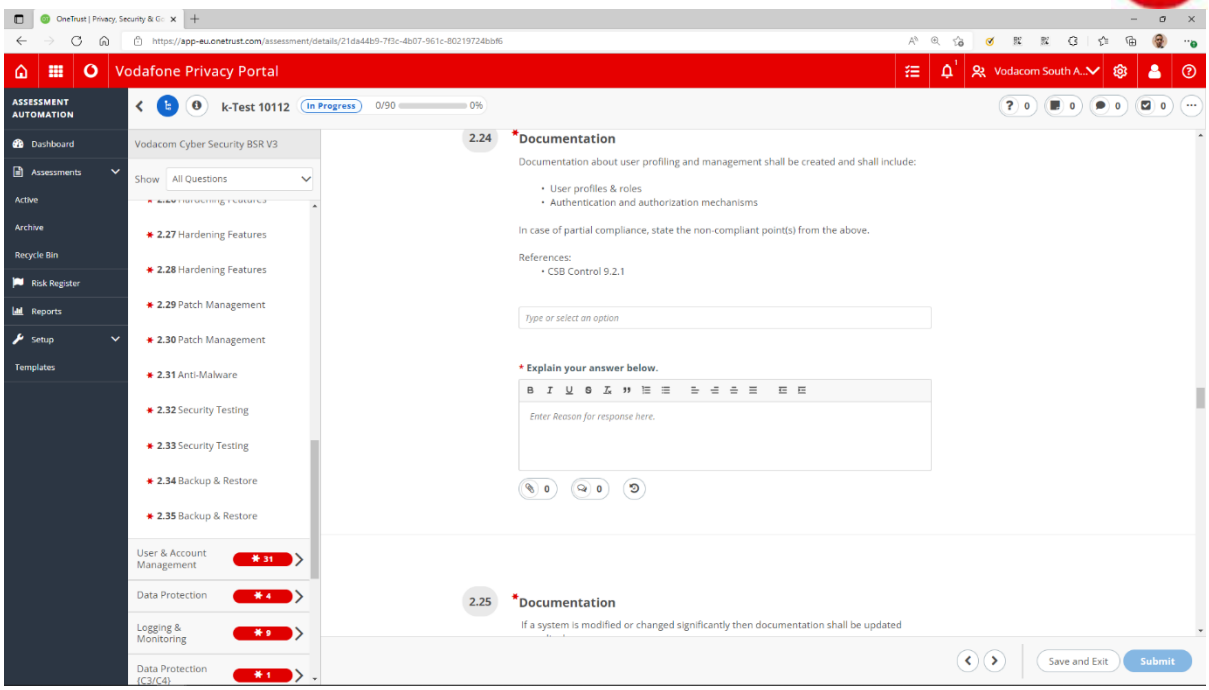


Figure 44

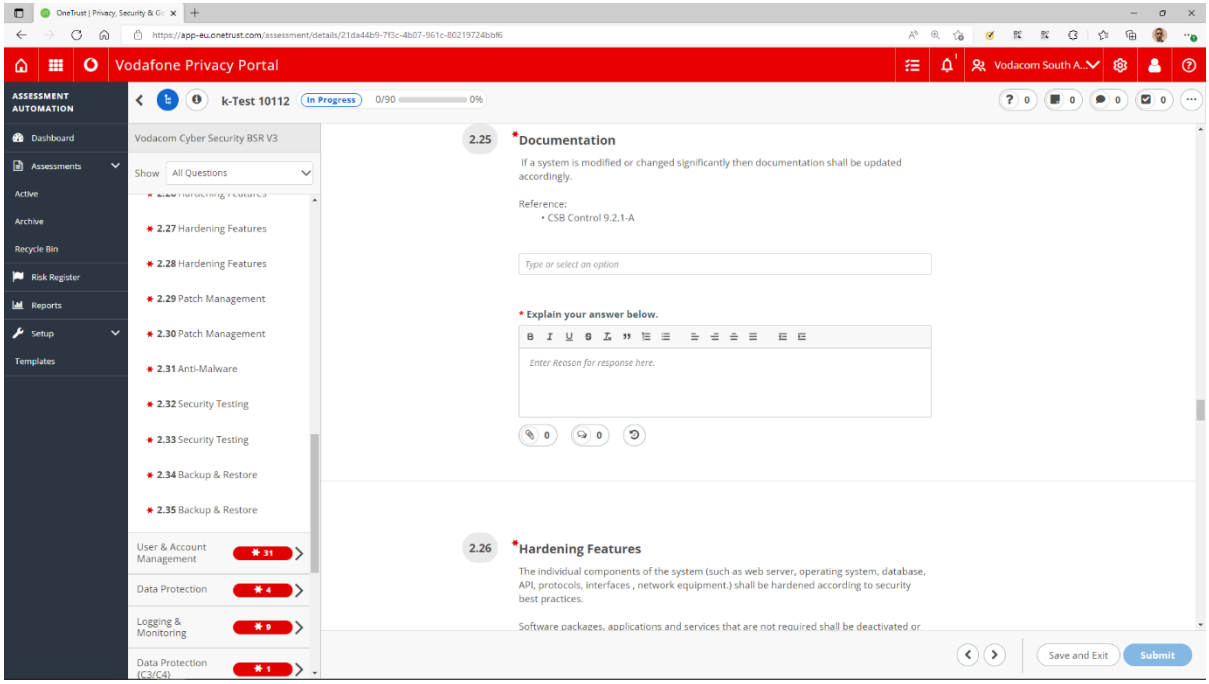


Figure 45

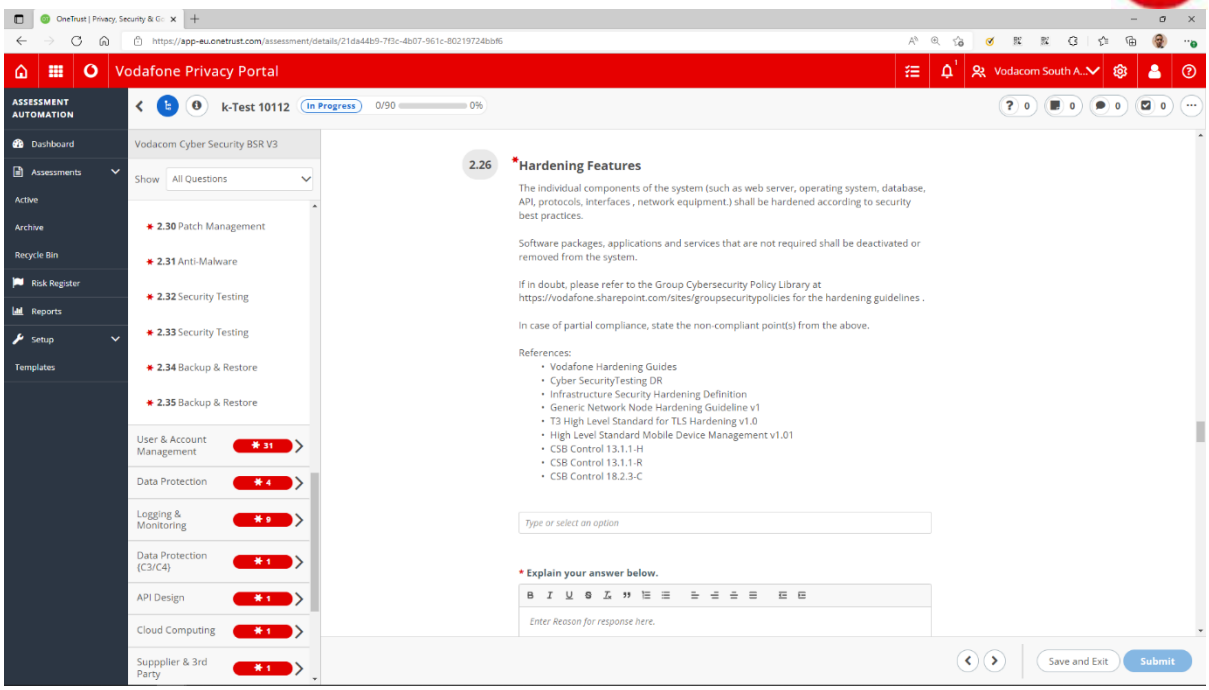


Figure 46

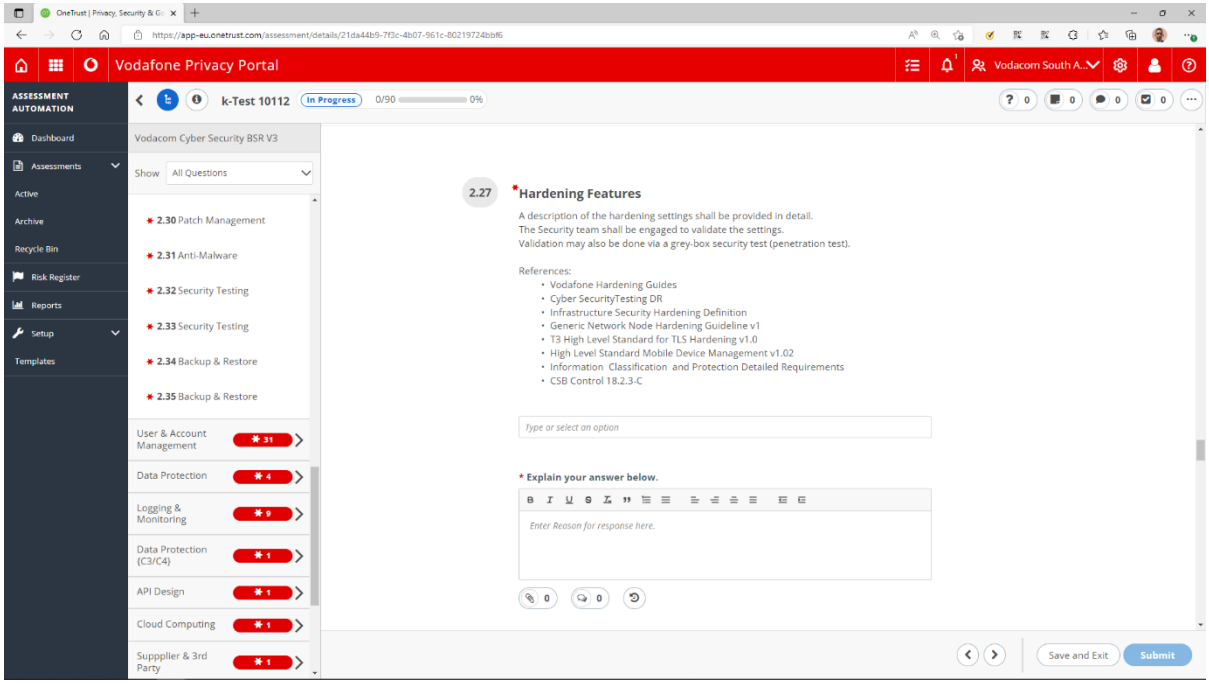


Figure 47

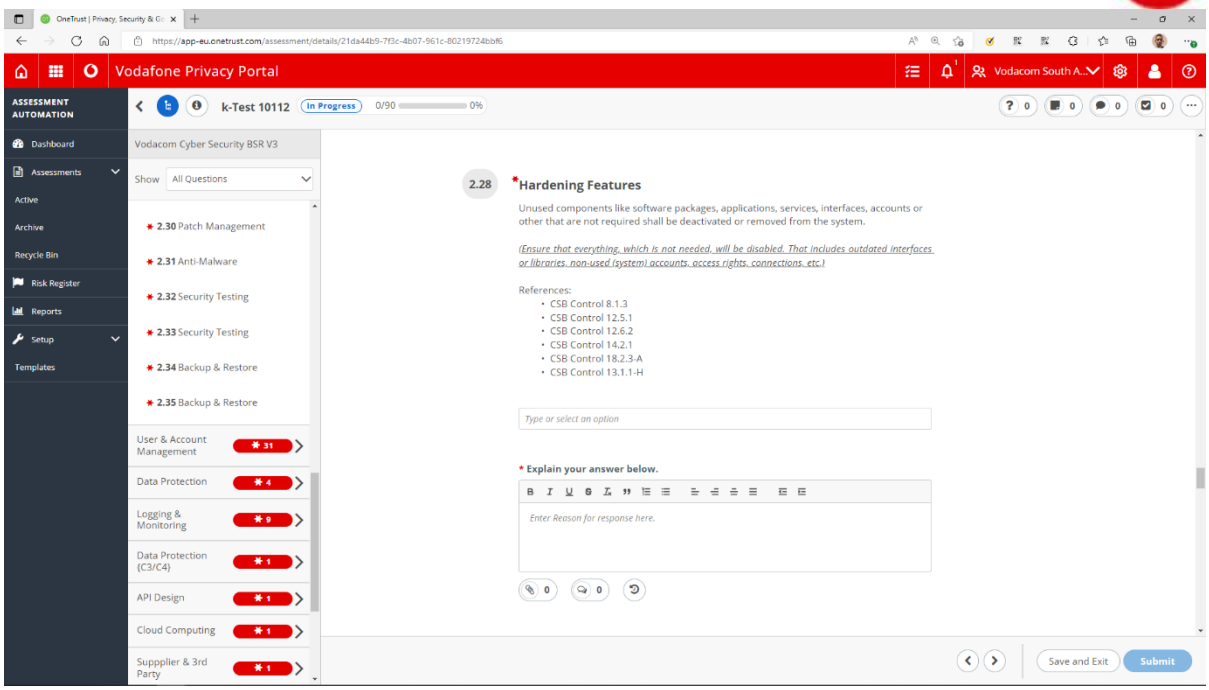


Figure 48

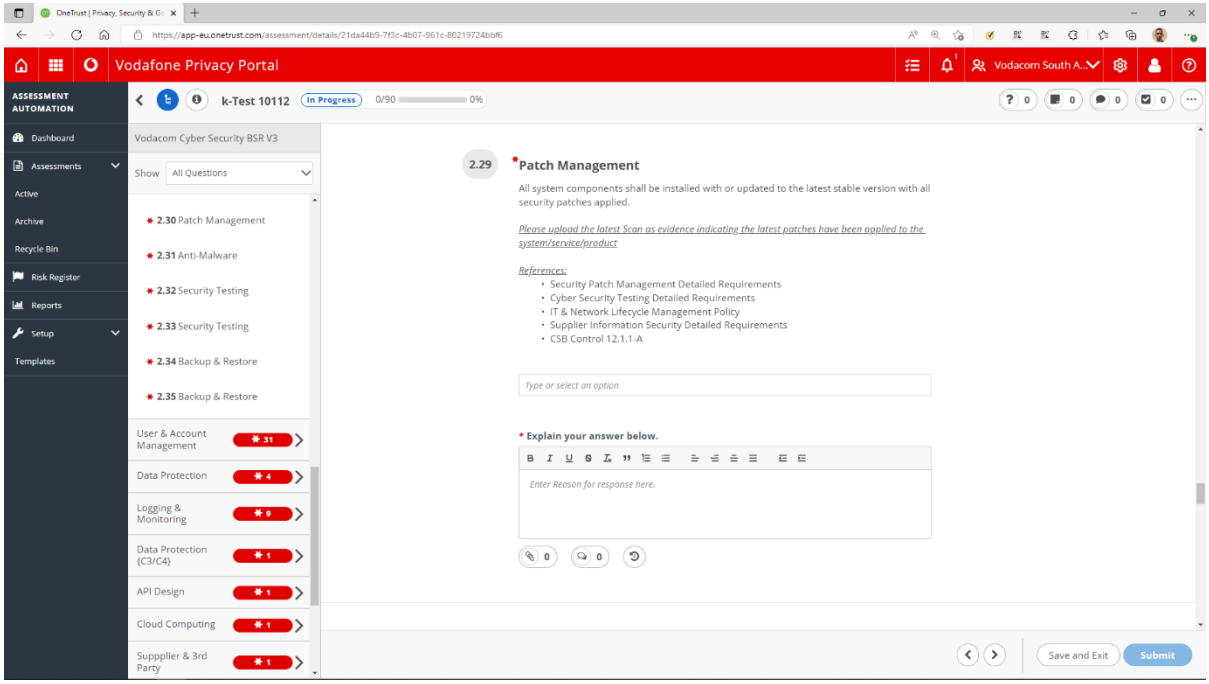


Figure 49

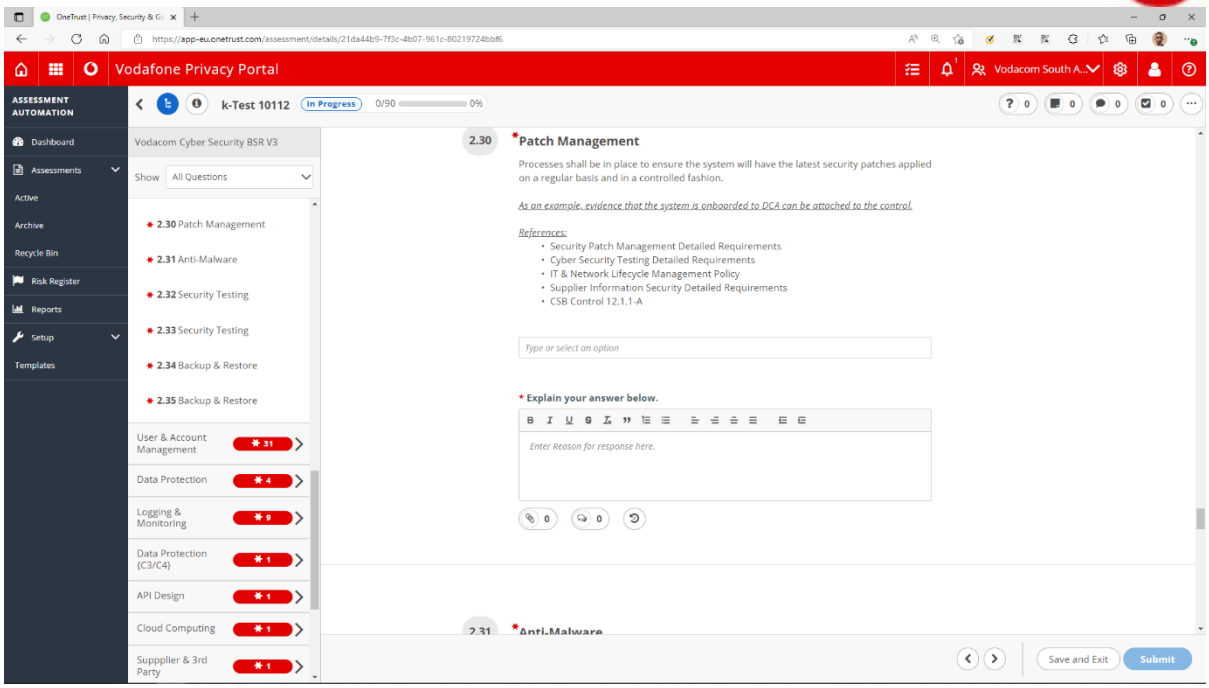


Figure 50

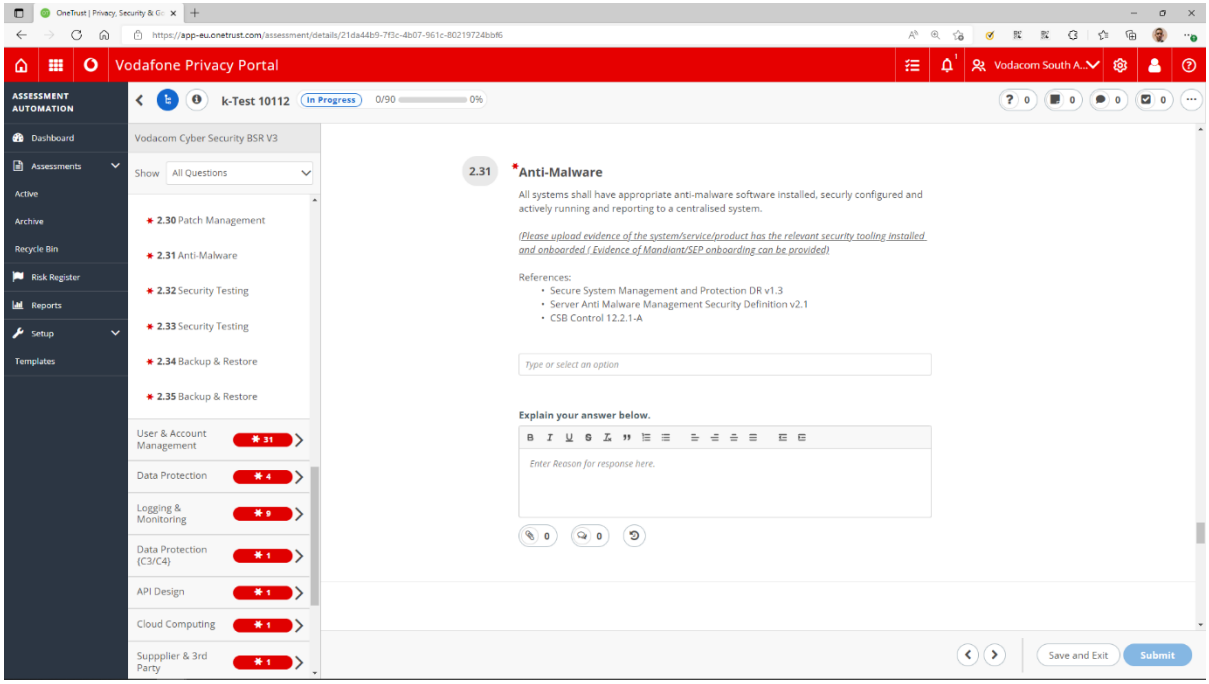


Figure 51

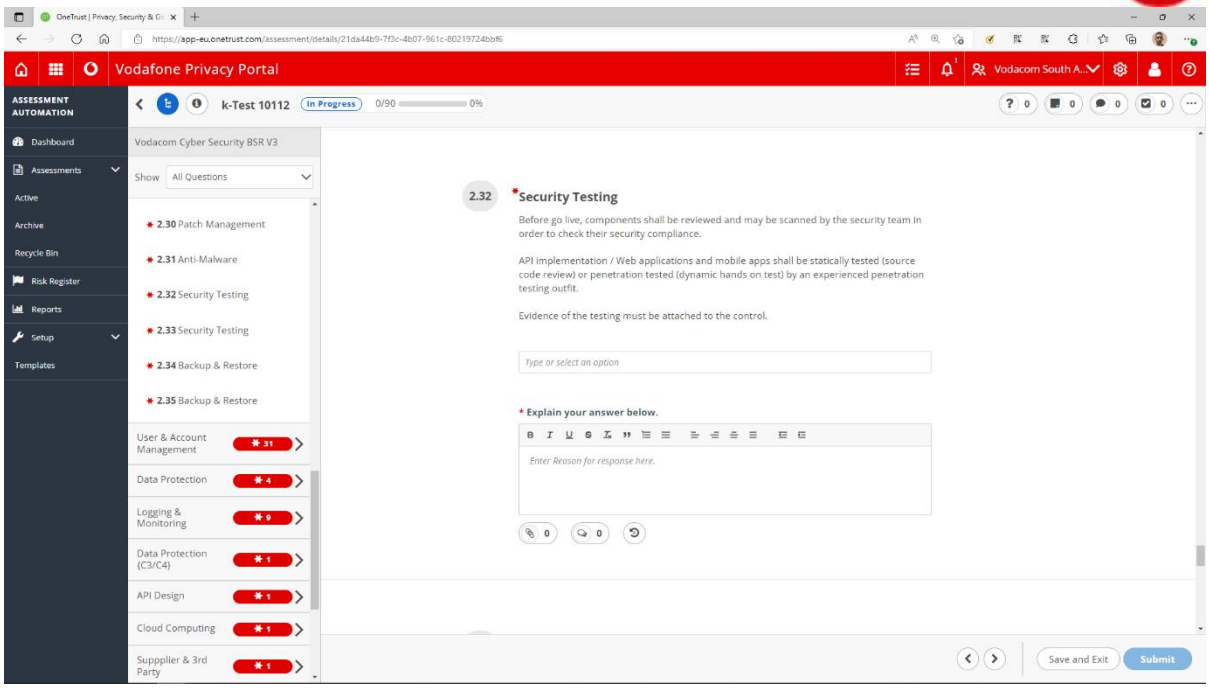


Figure 52

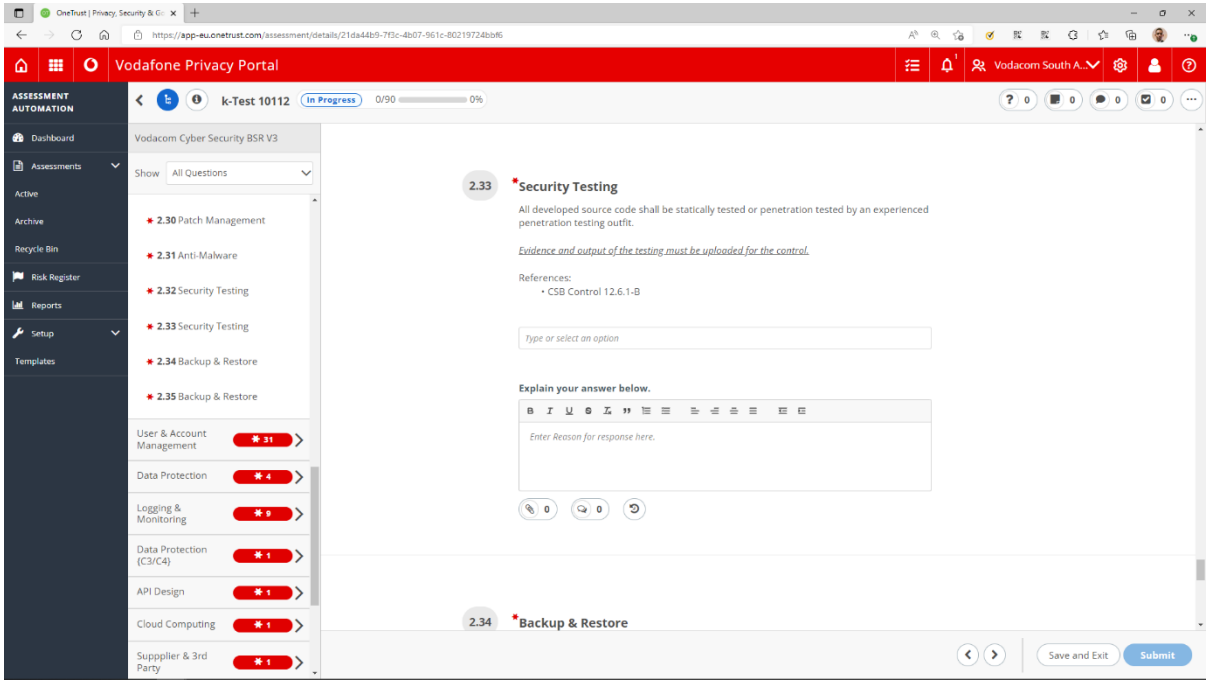


Figure 53

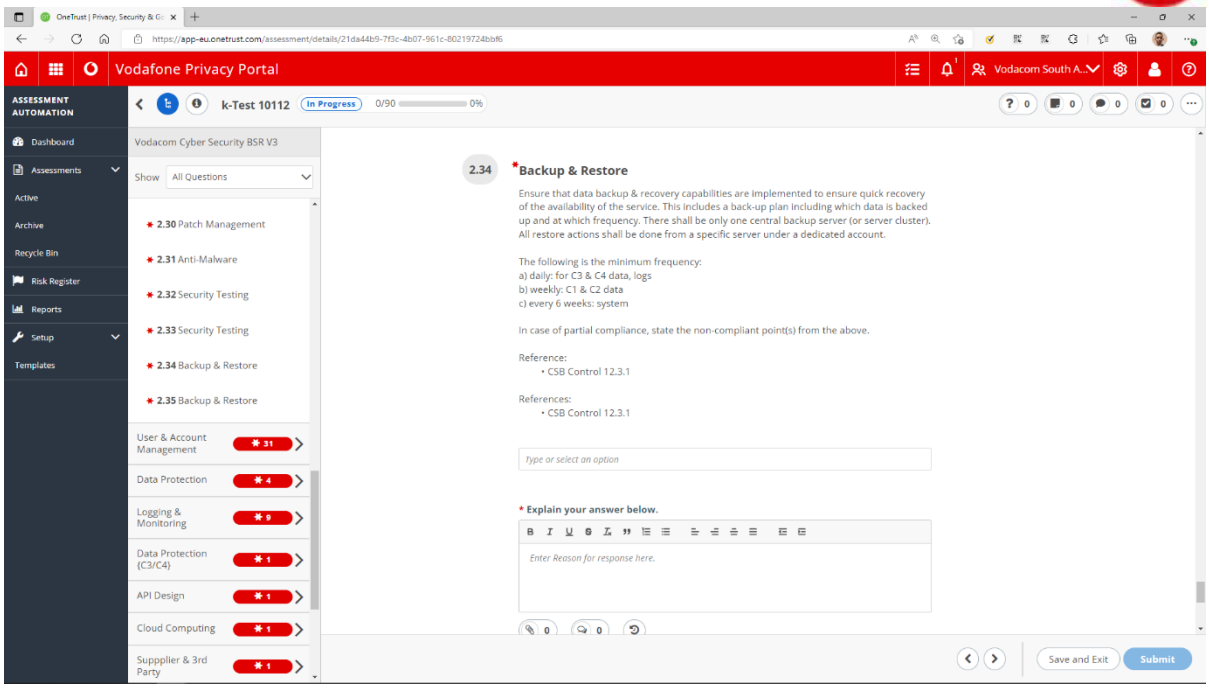


Figure 54

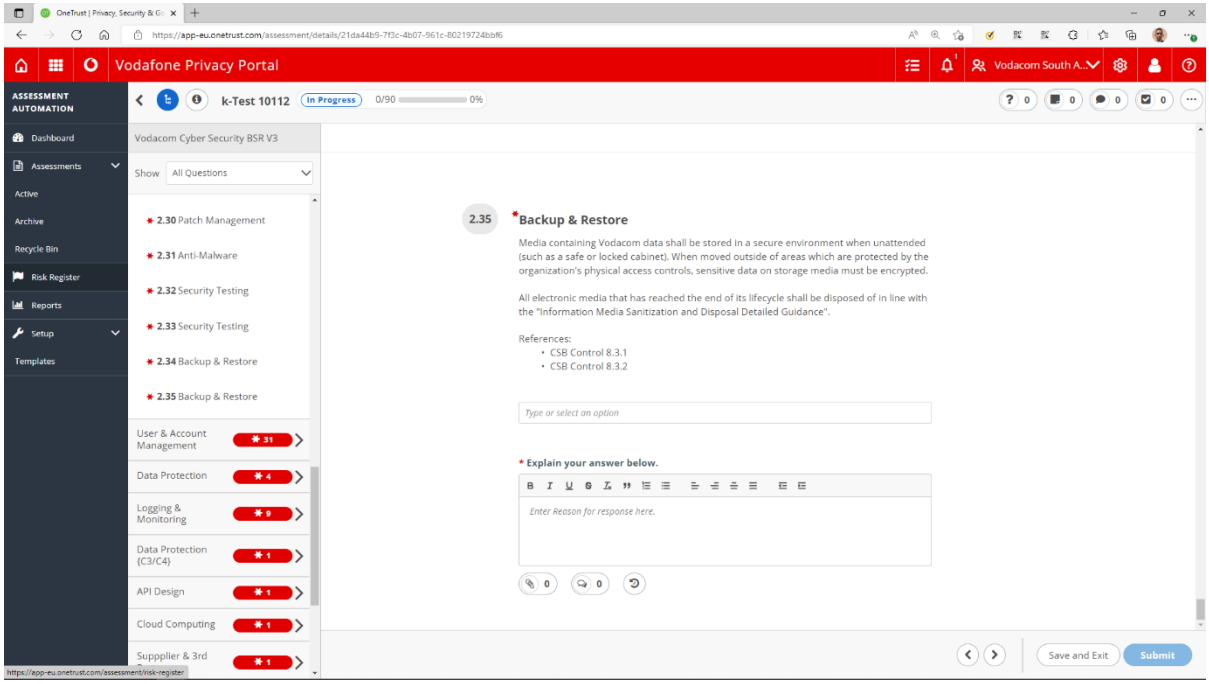


Figure 55

5.3 User and Account Management

Questions 3.1 to 3.31

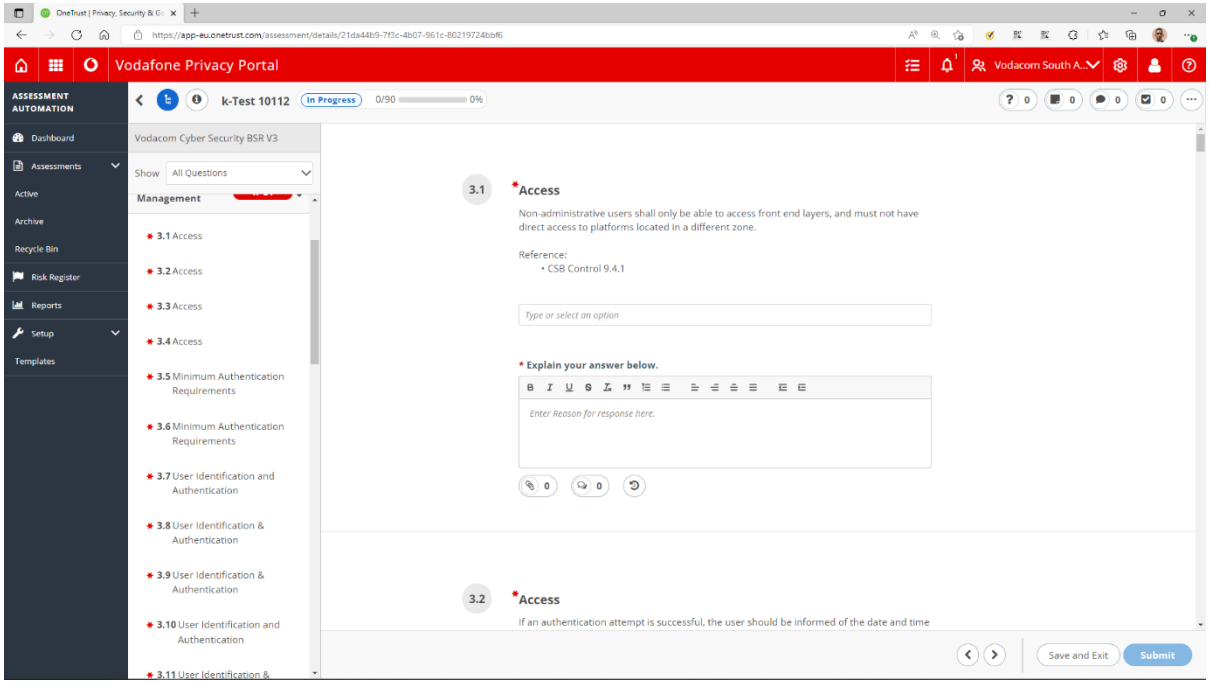


Figure 56

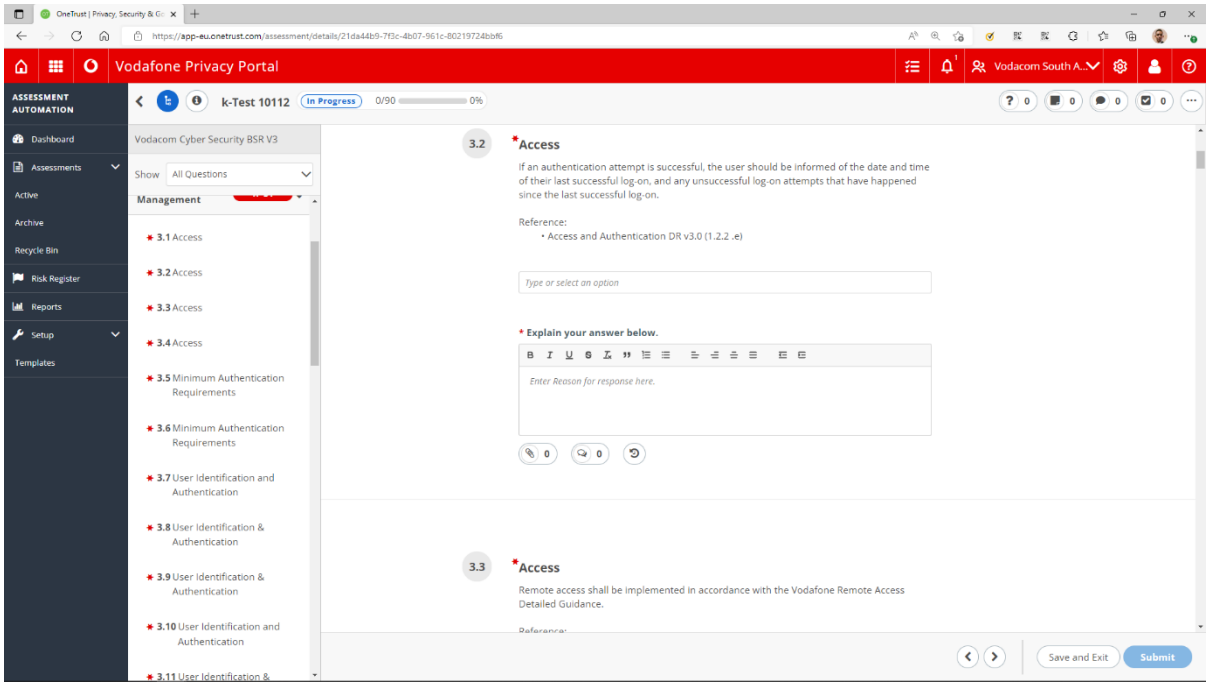


Figure 57

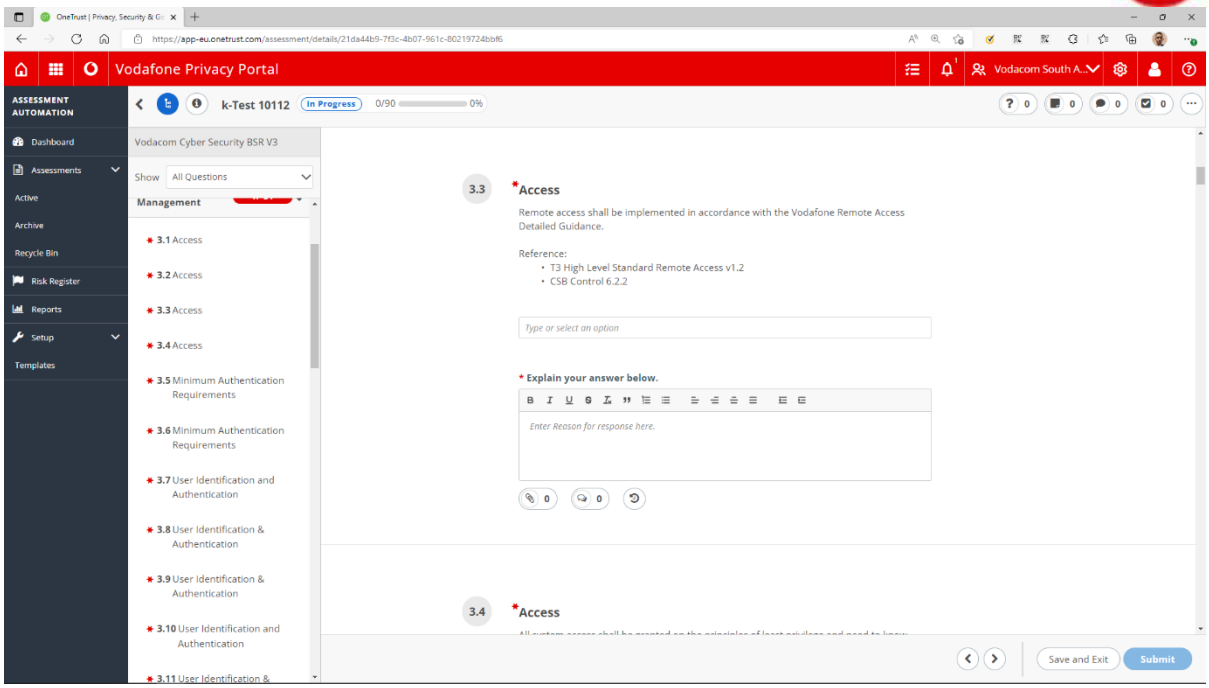


Figure 58

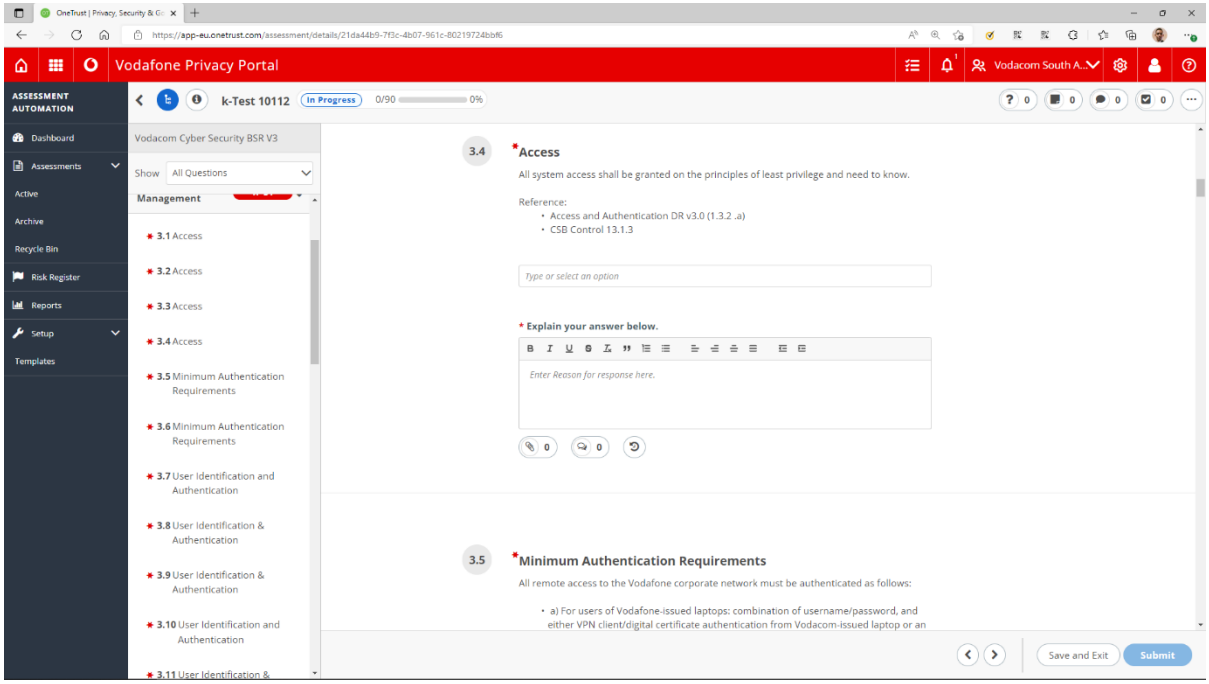


Figure 59

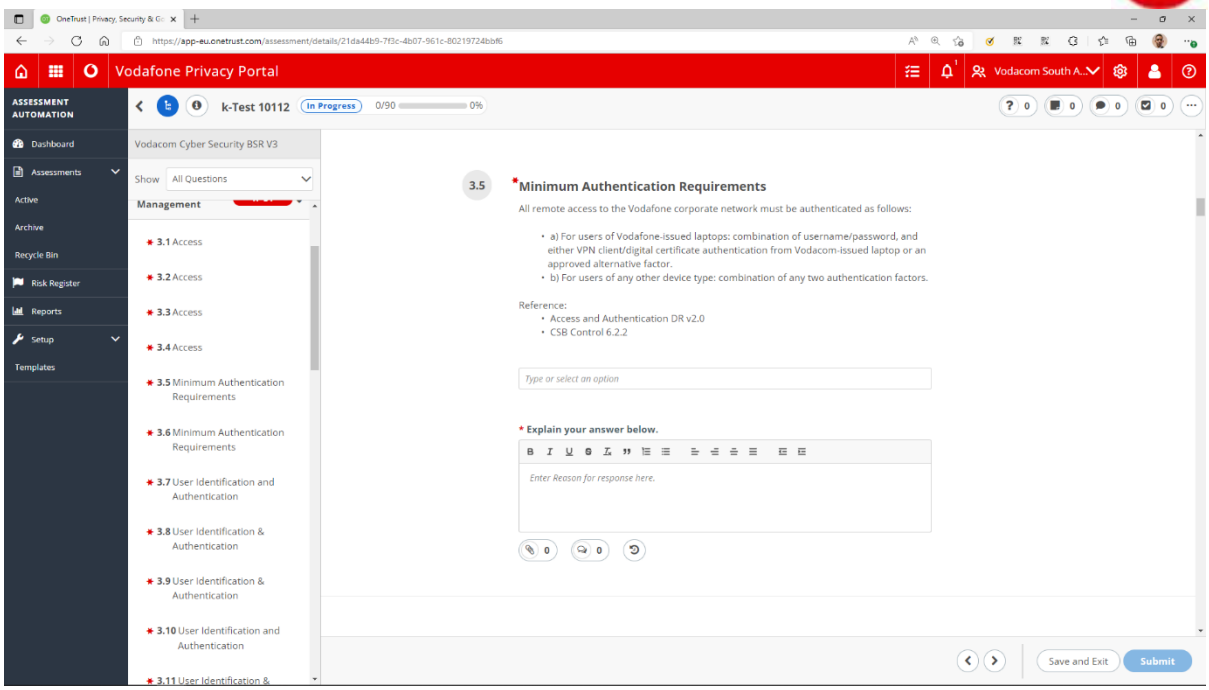


Figure 60

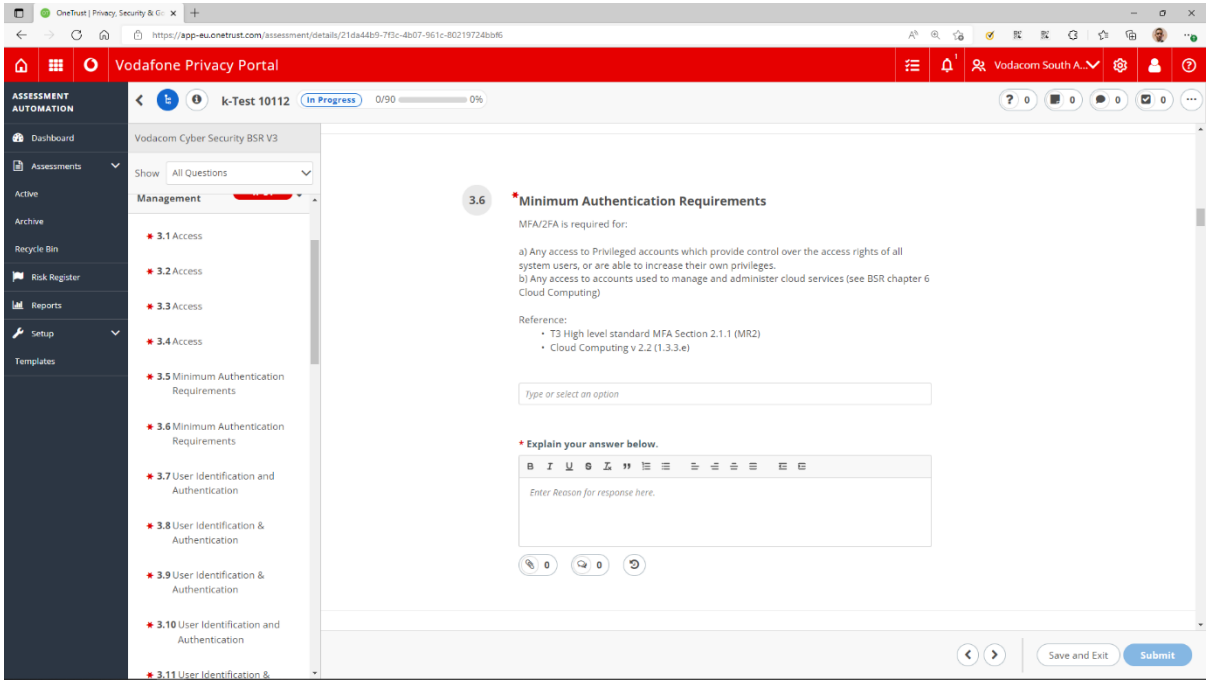


Figure 61

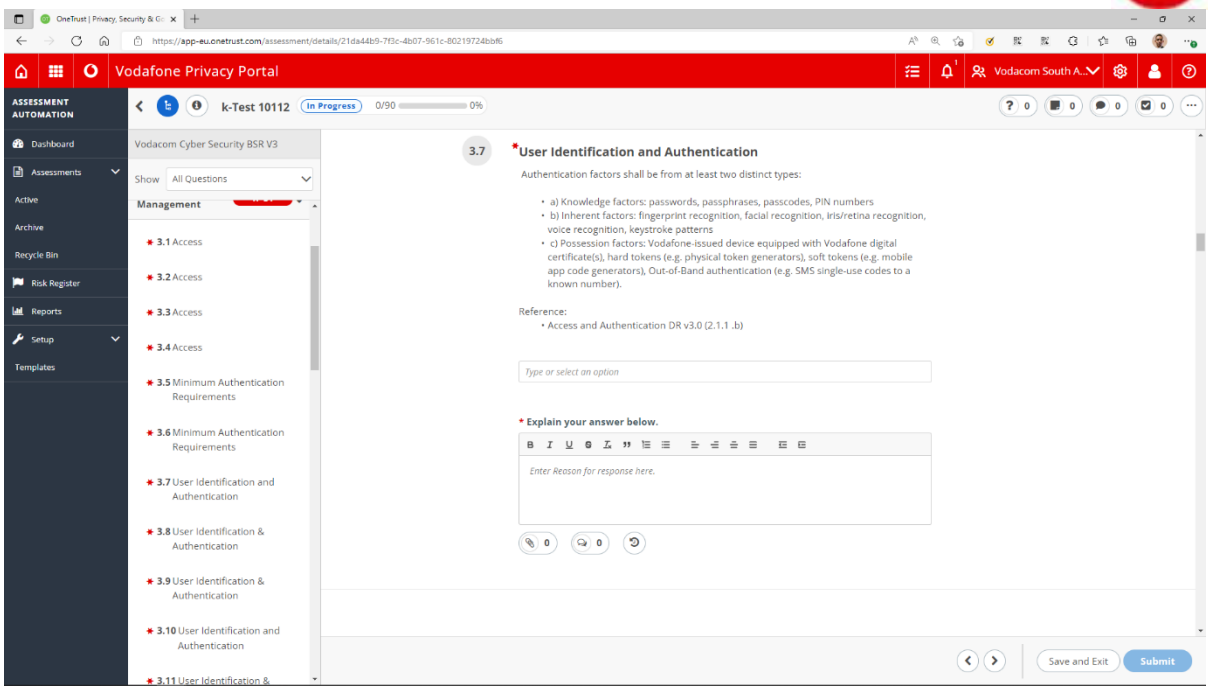


Figure 62

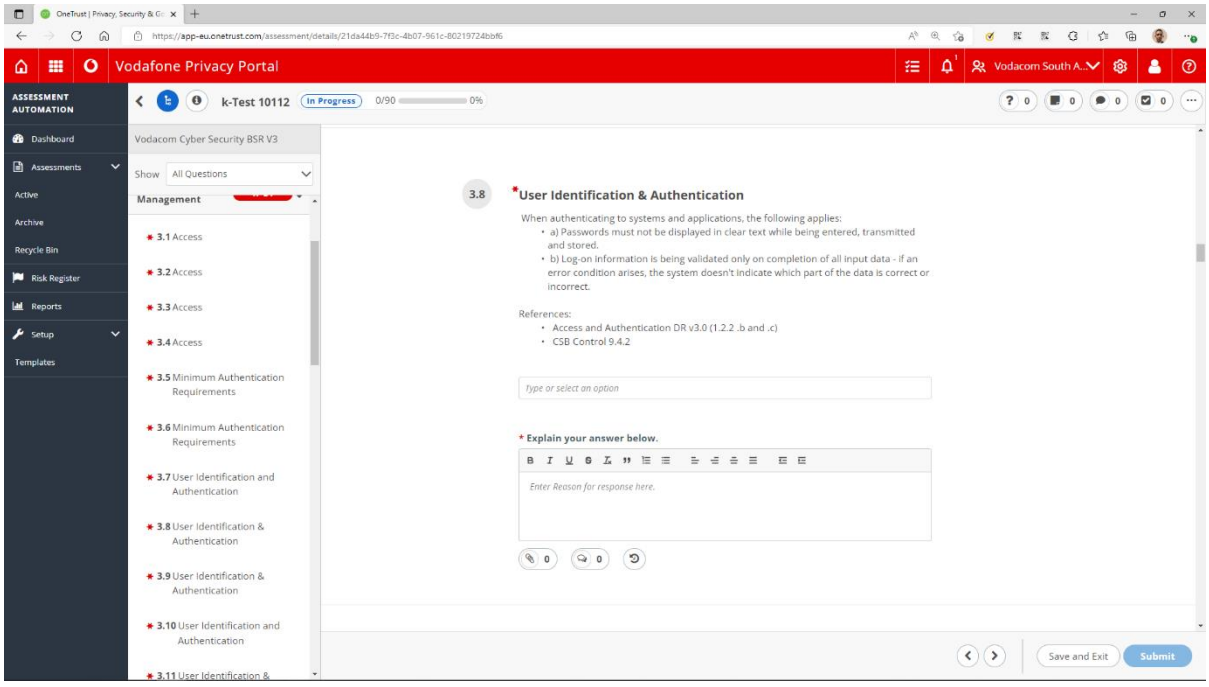


Figure 63

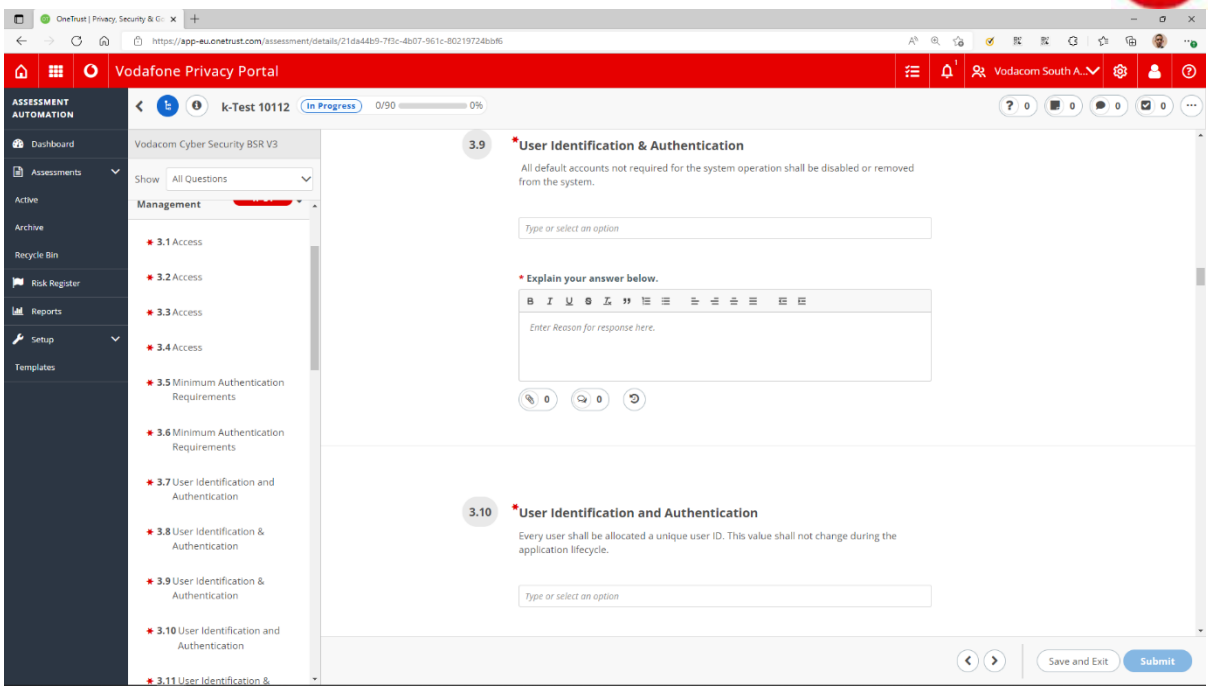


Figure 64

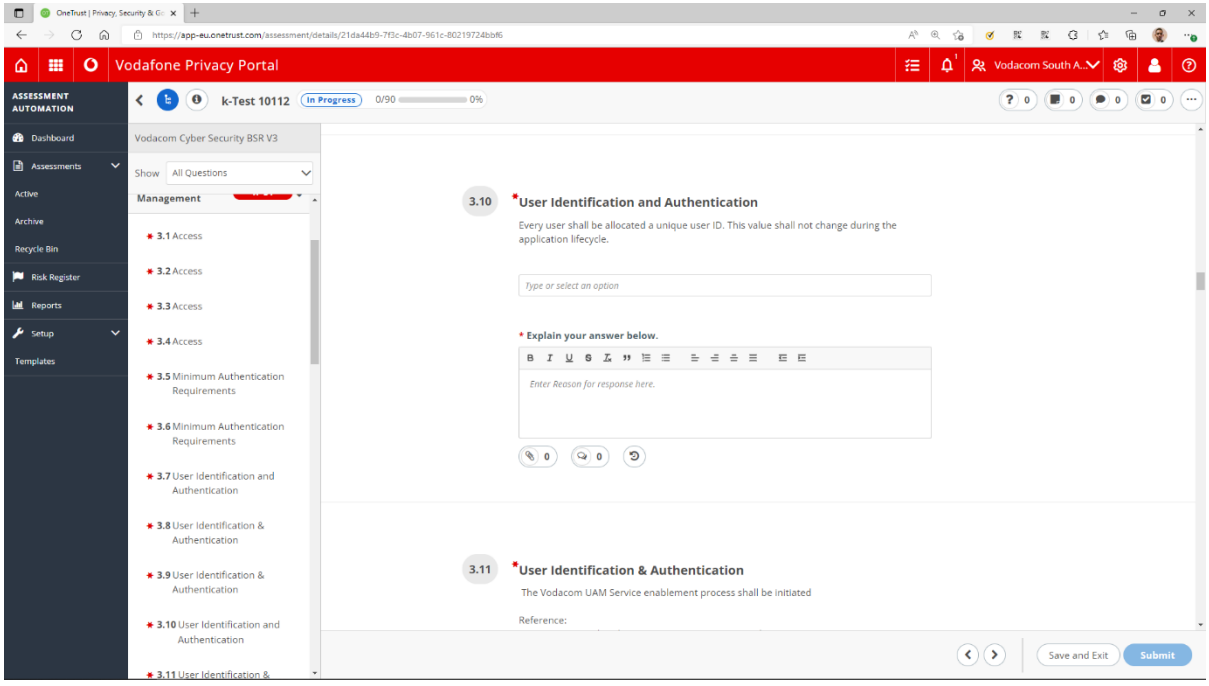


Figure 65

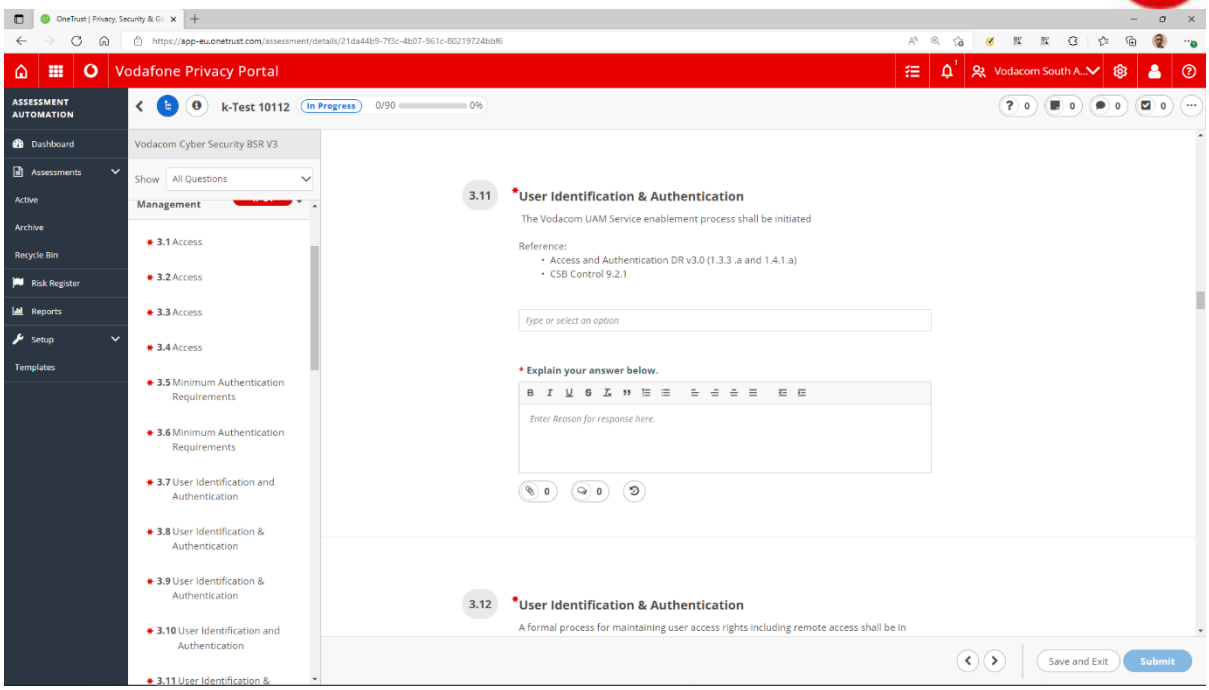


Figure 66

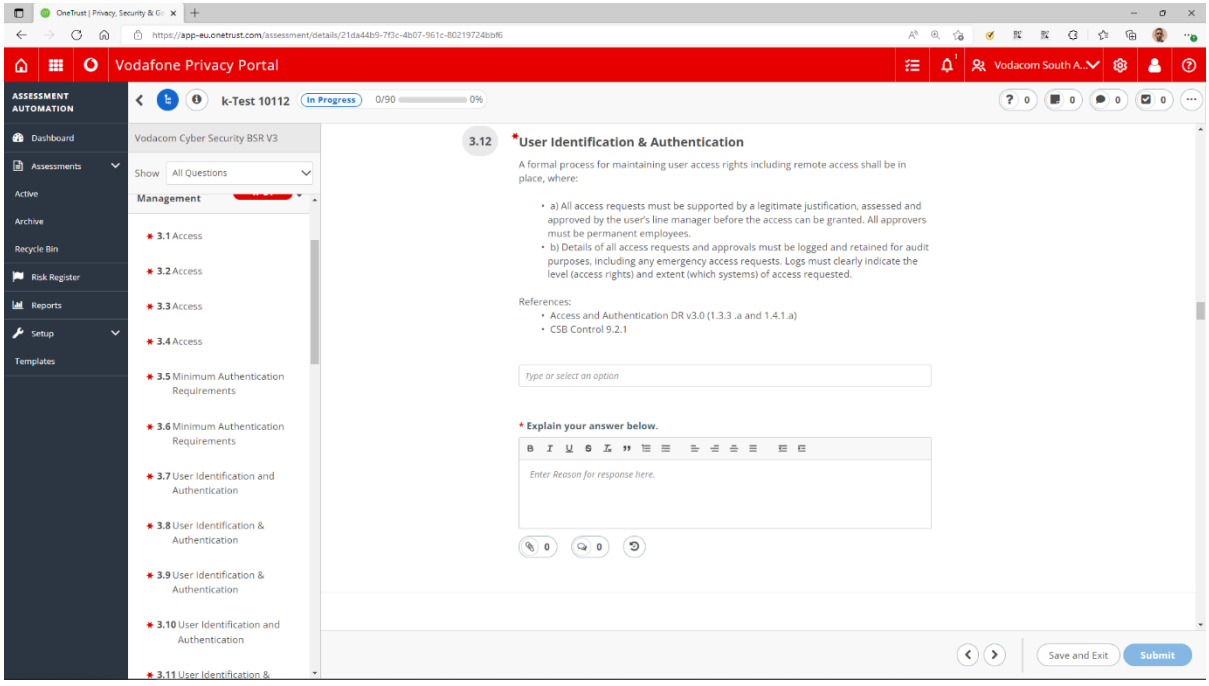


Figure 67

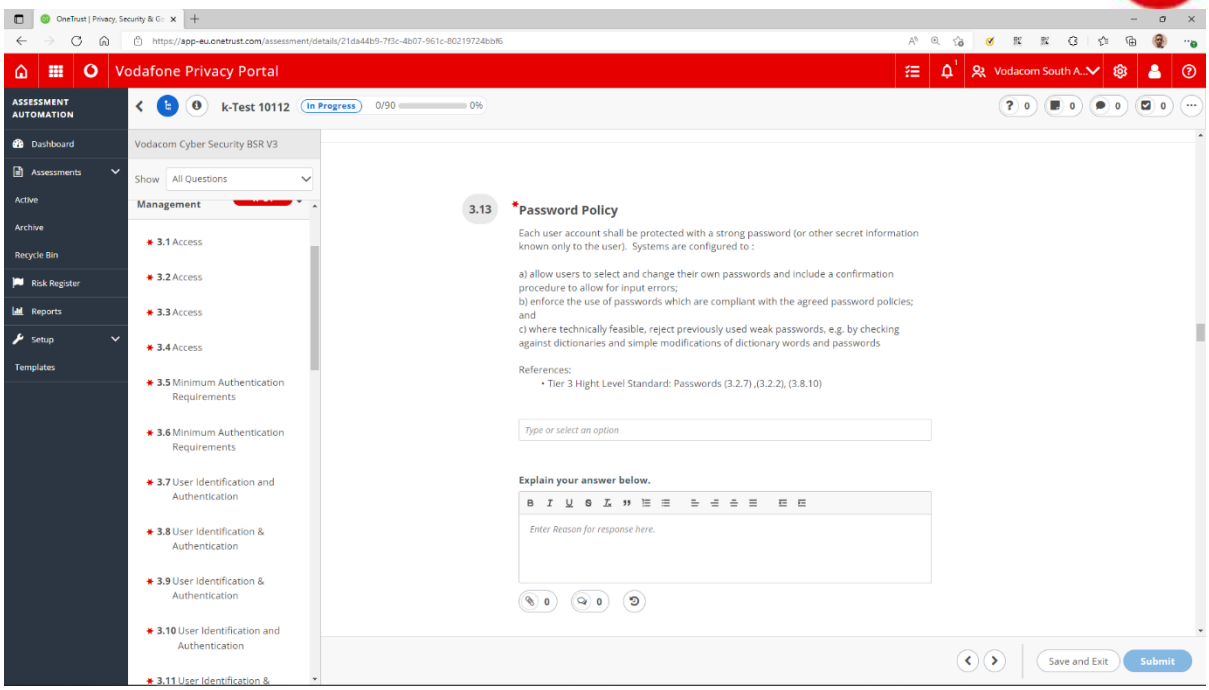


Figure 68

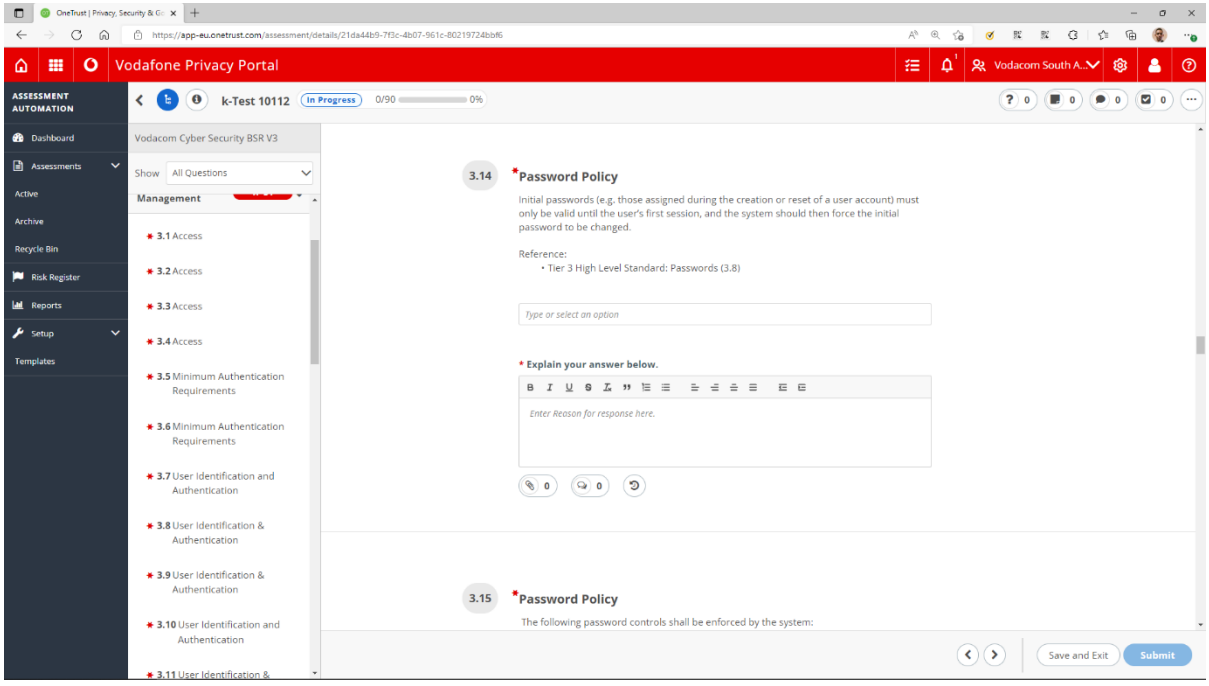


Figure 69

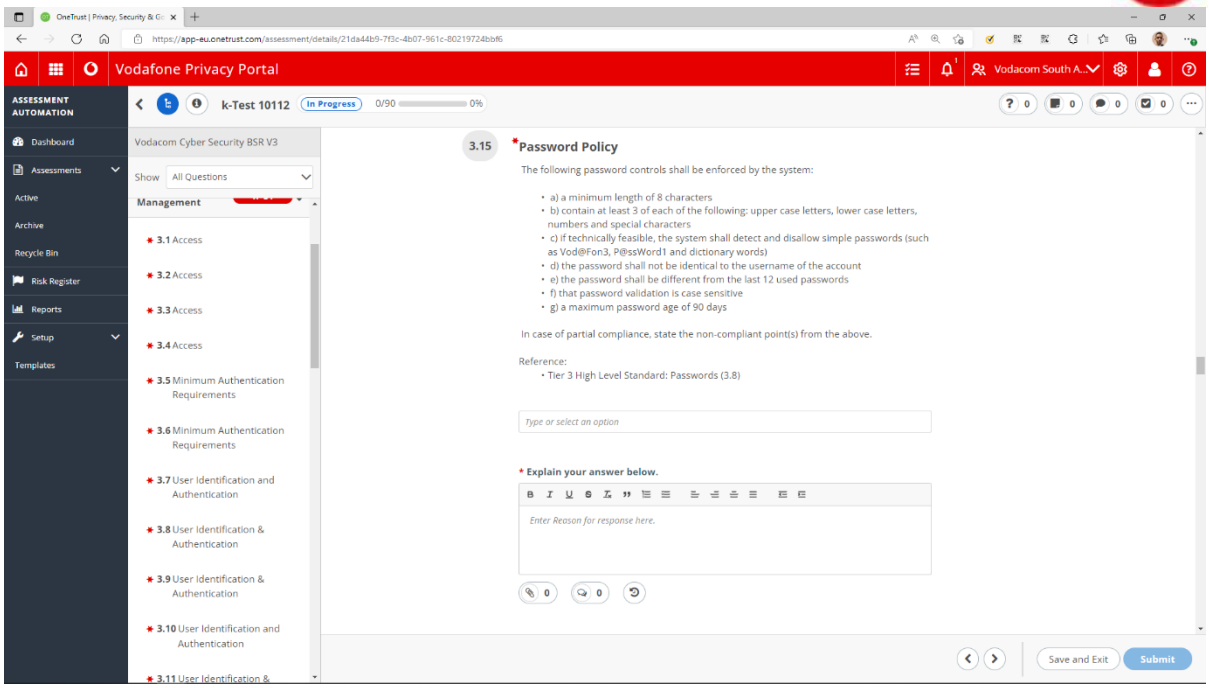


Figure 70

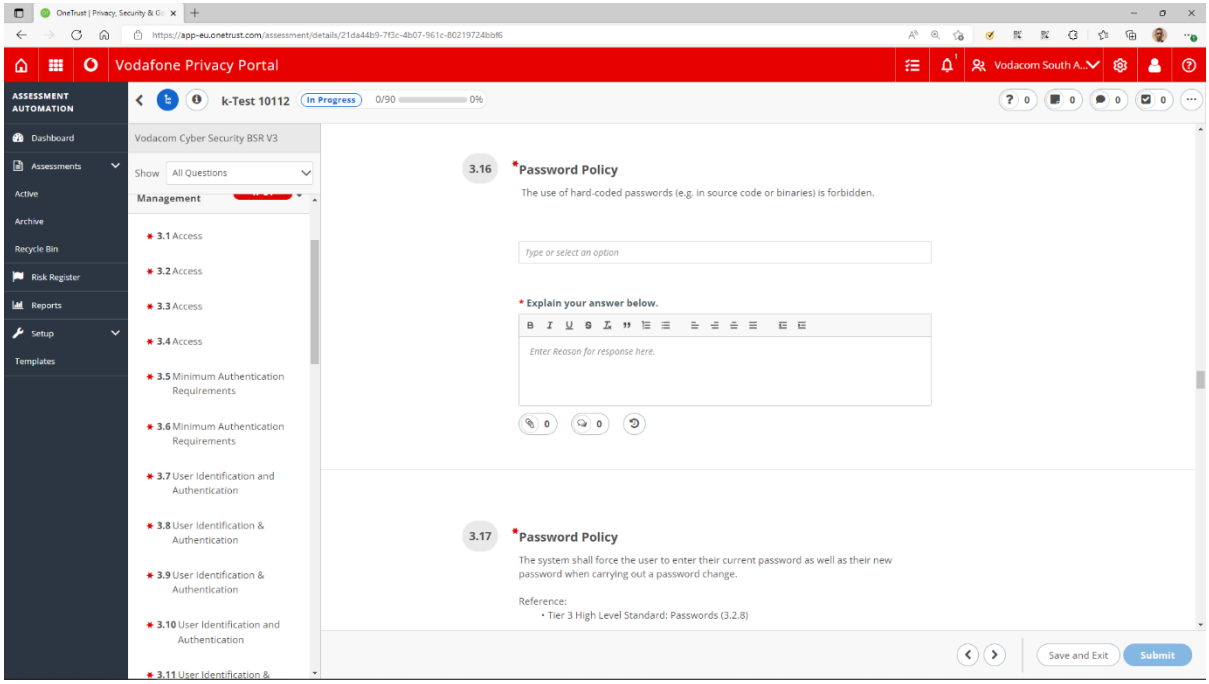


Figure 71

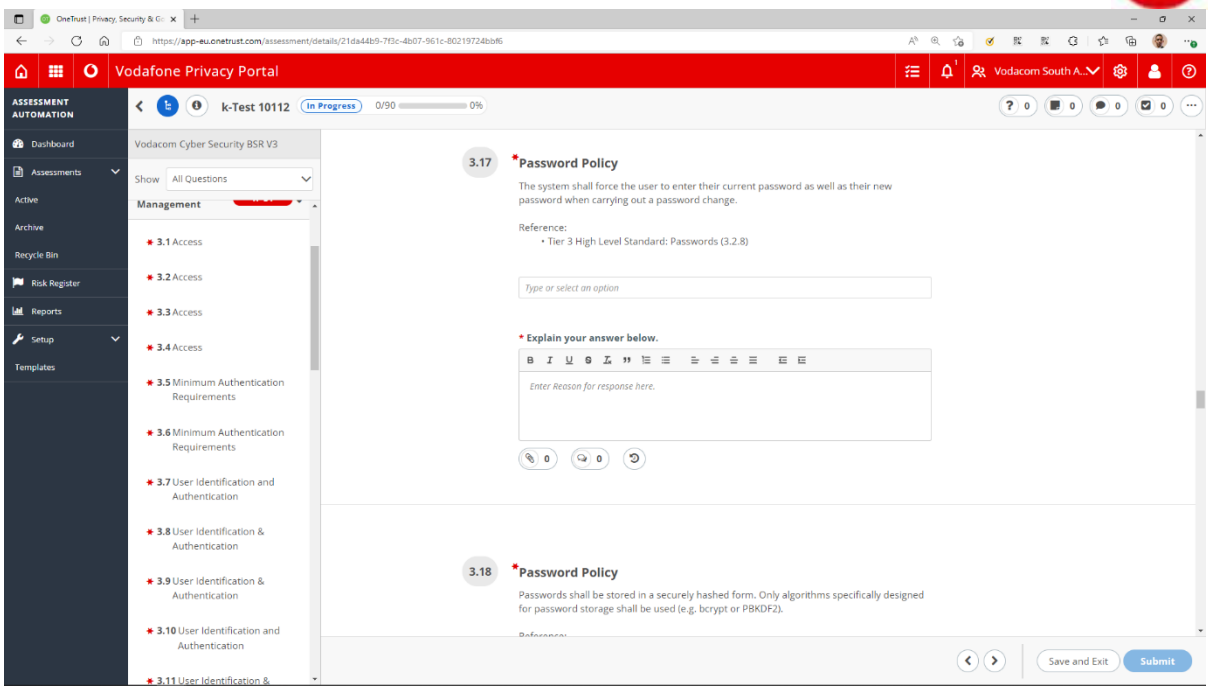


Figure 72

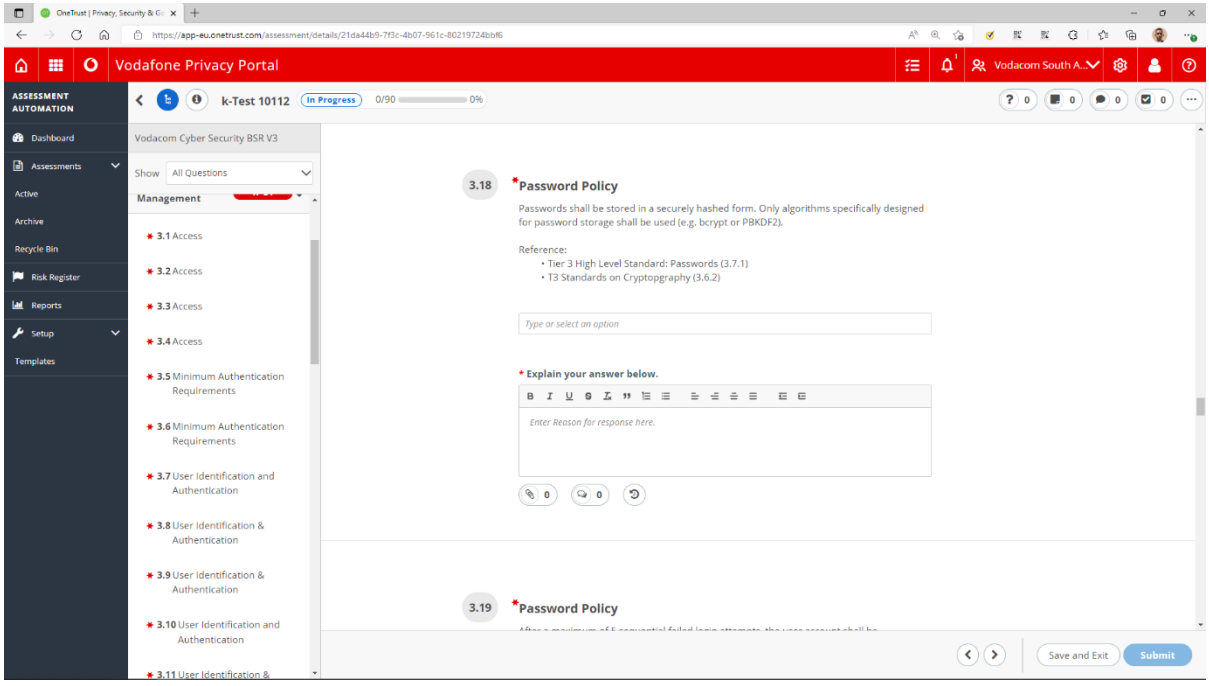


Figure 73

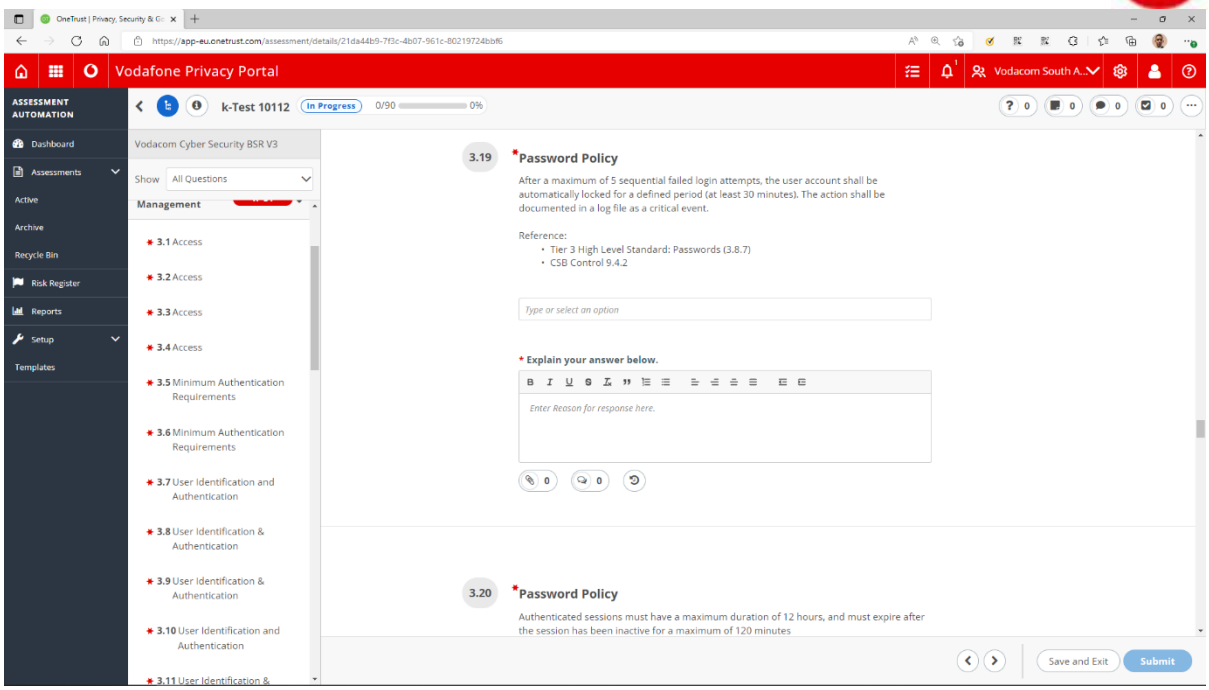


Figure 75

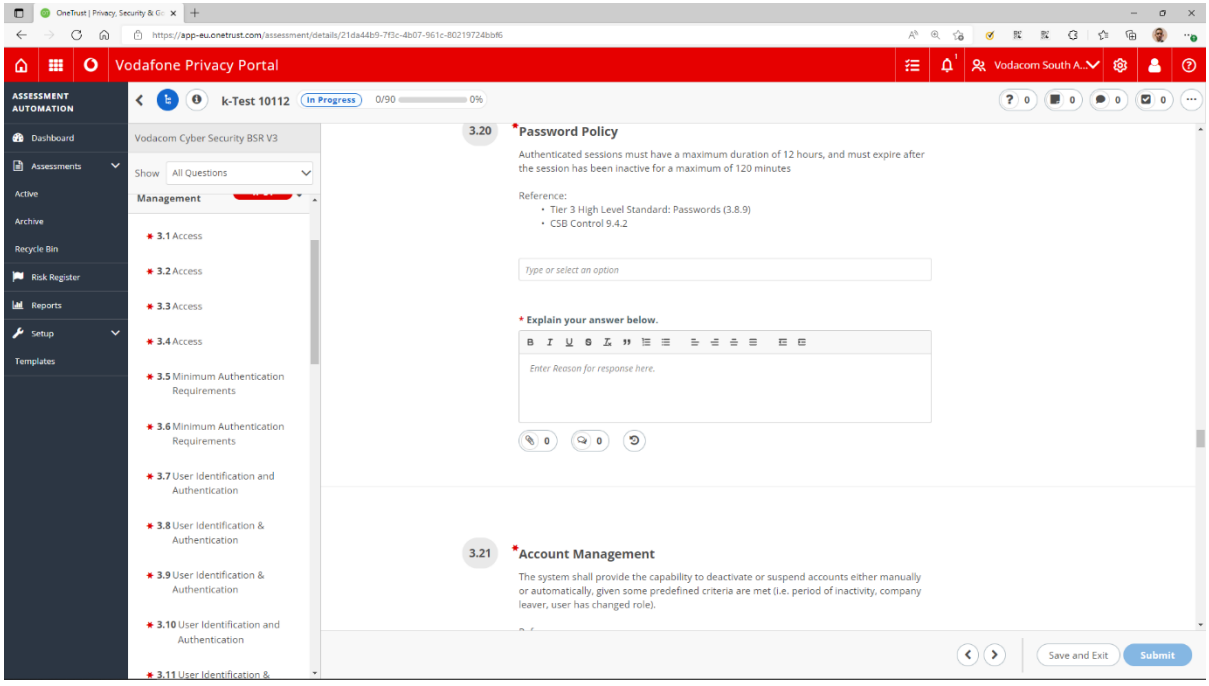


Figure 76

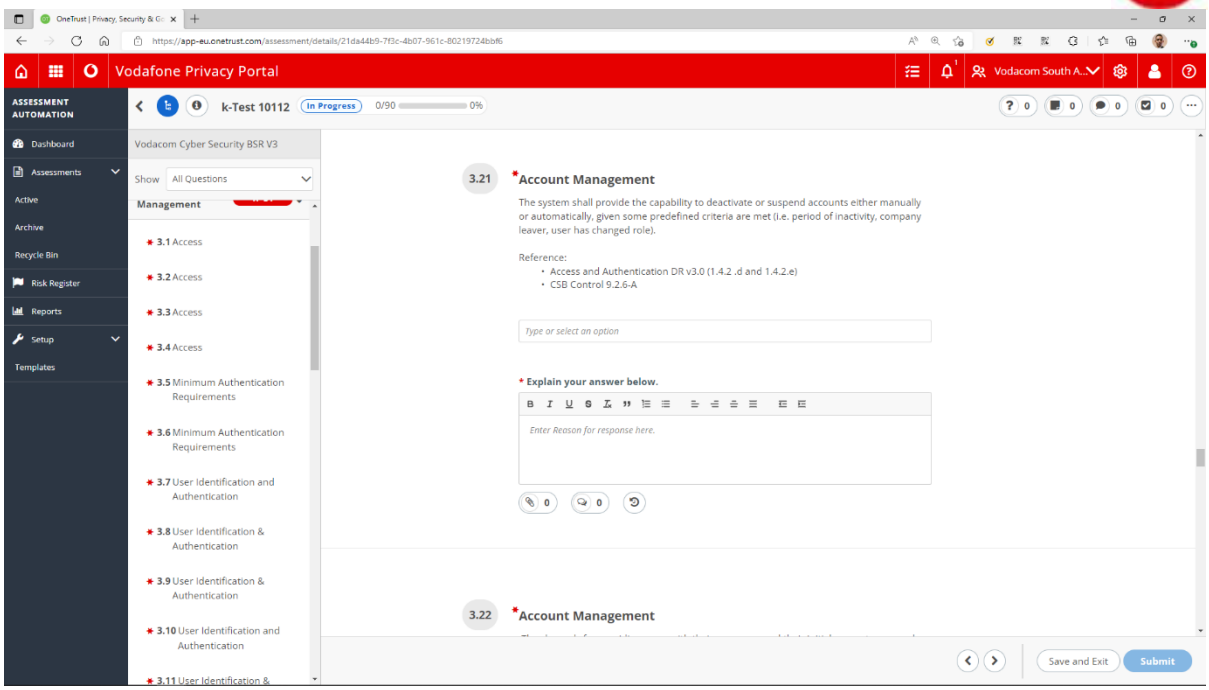


Figure 77

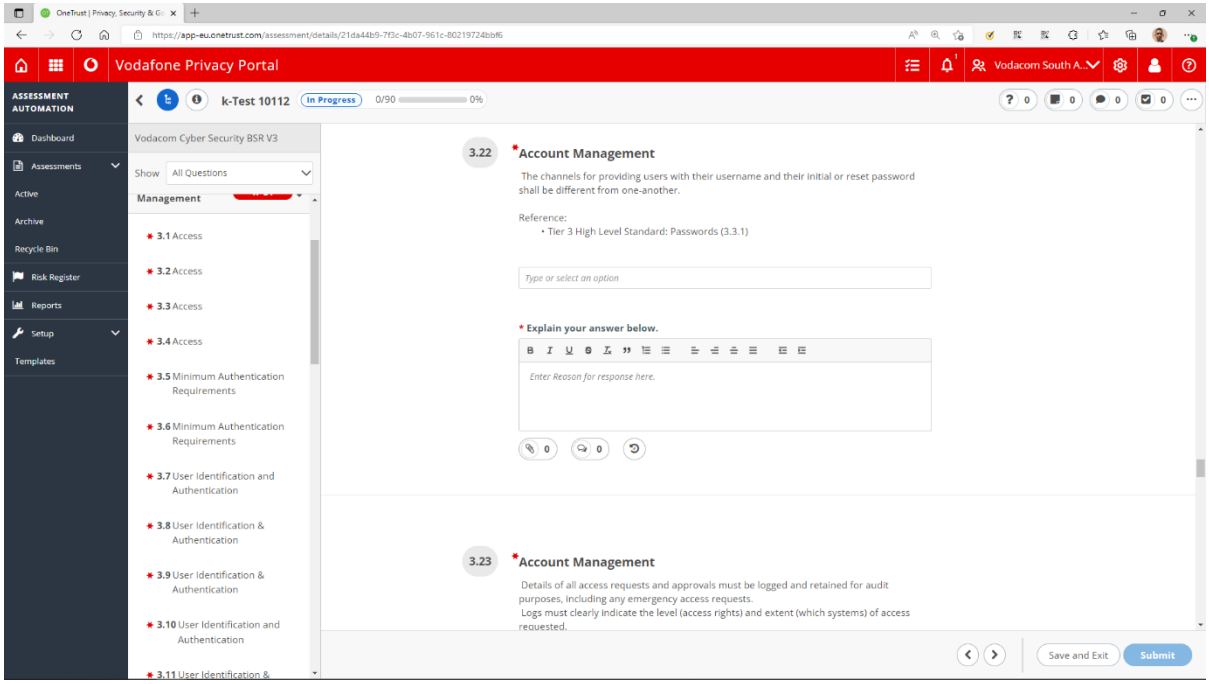


Figure 78

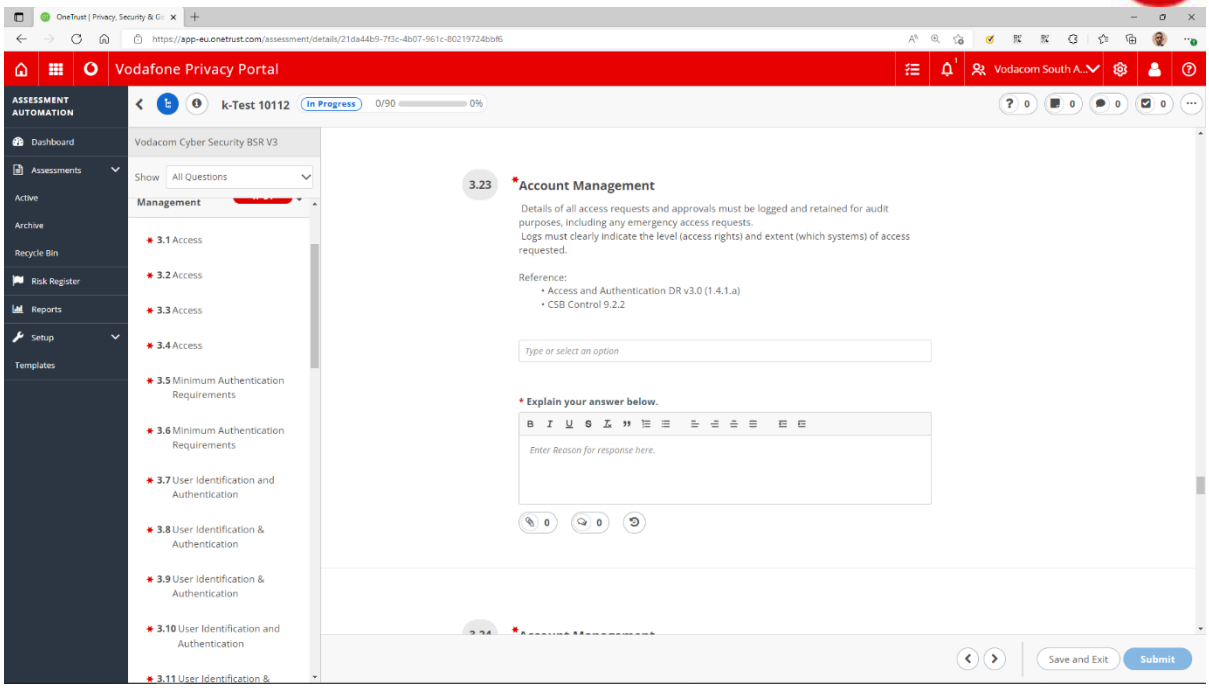


Figure 80

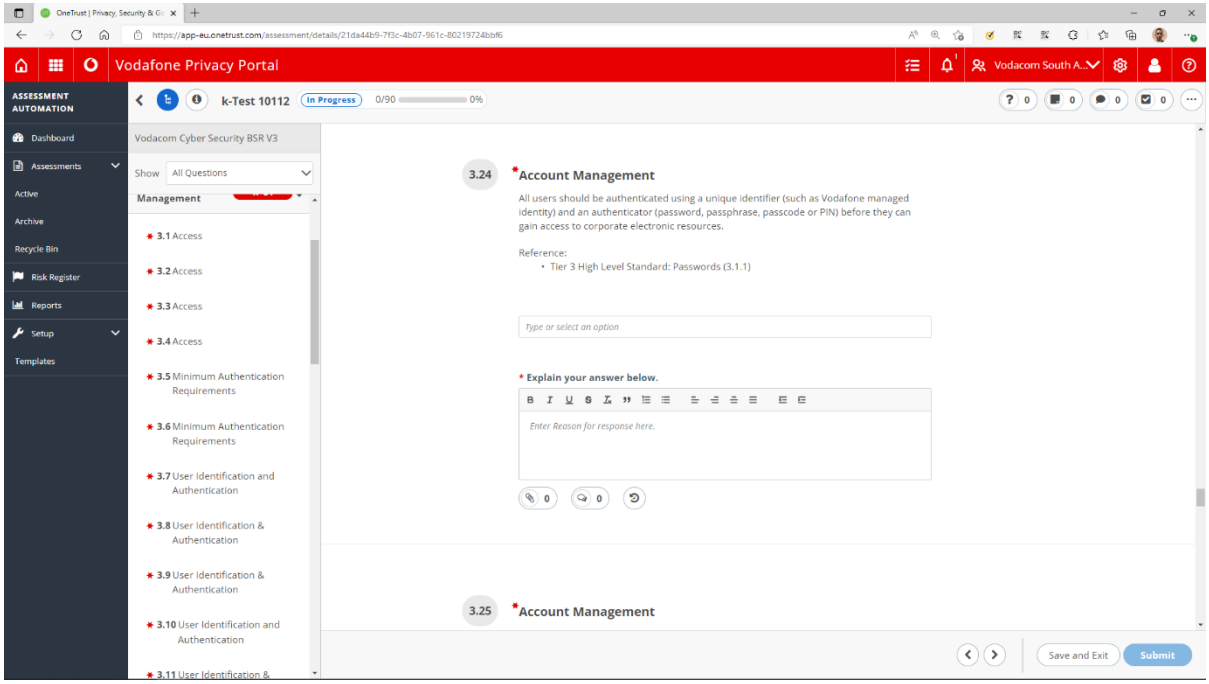


Figure 81

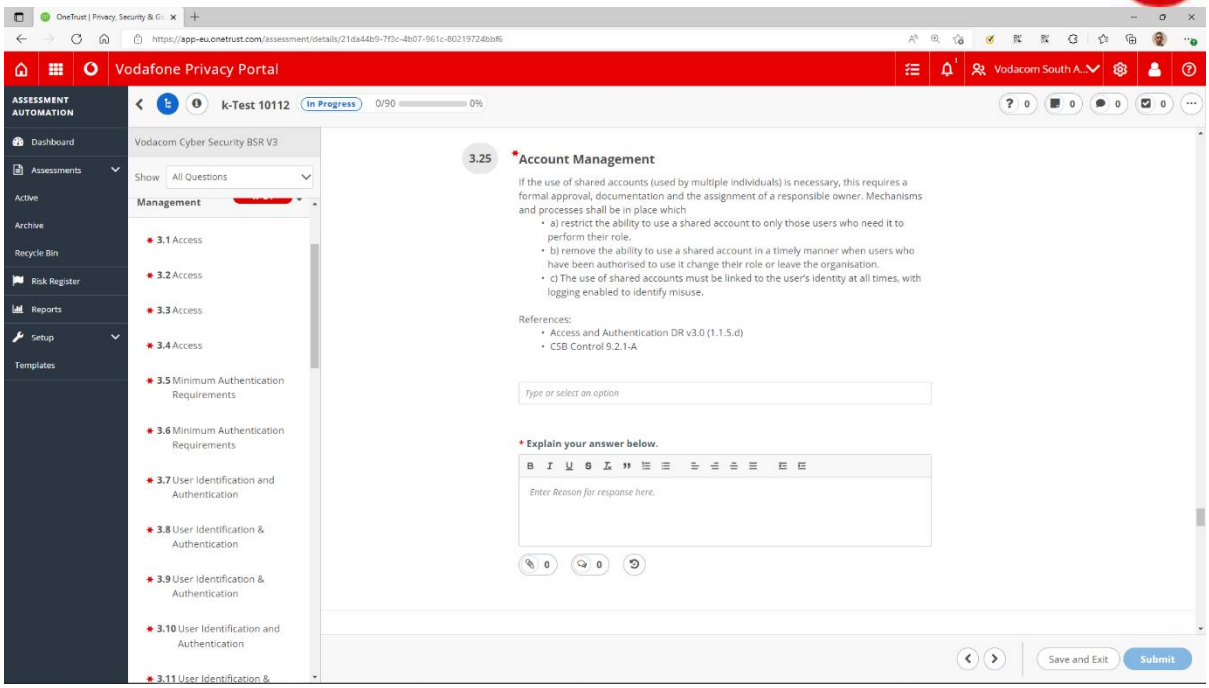


Figure 82

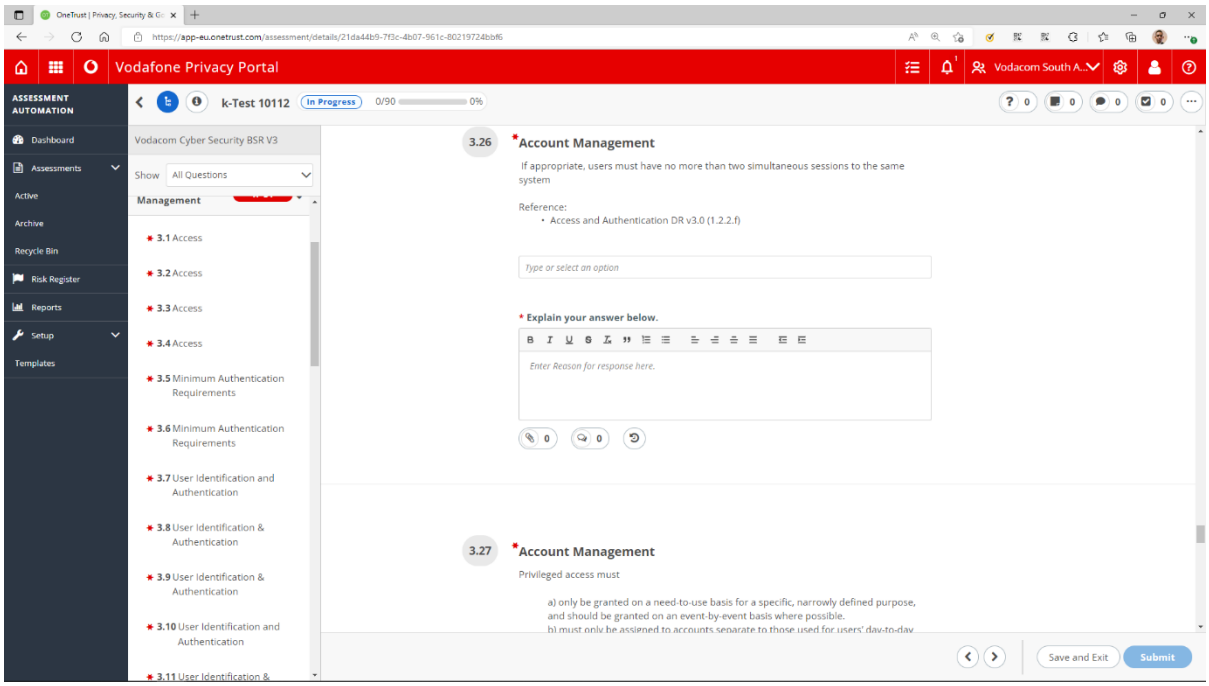


Figure 83

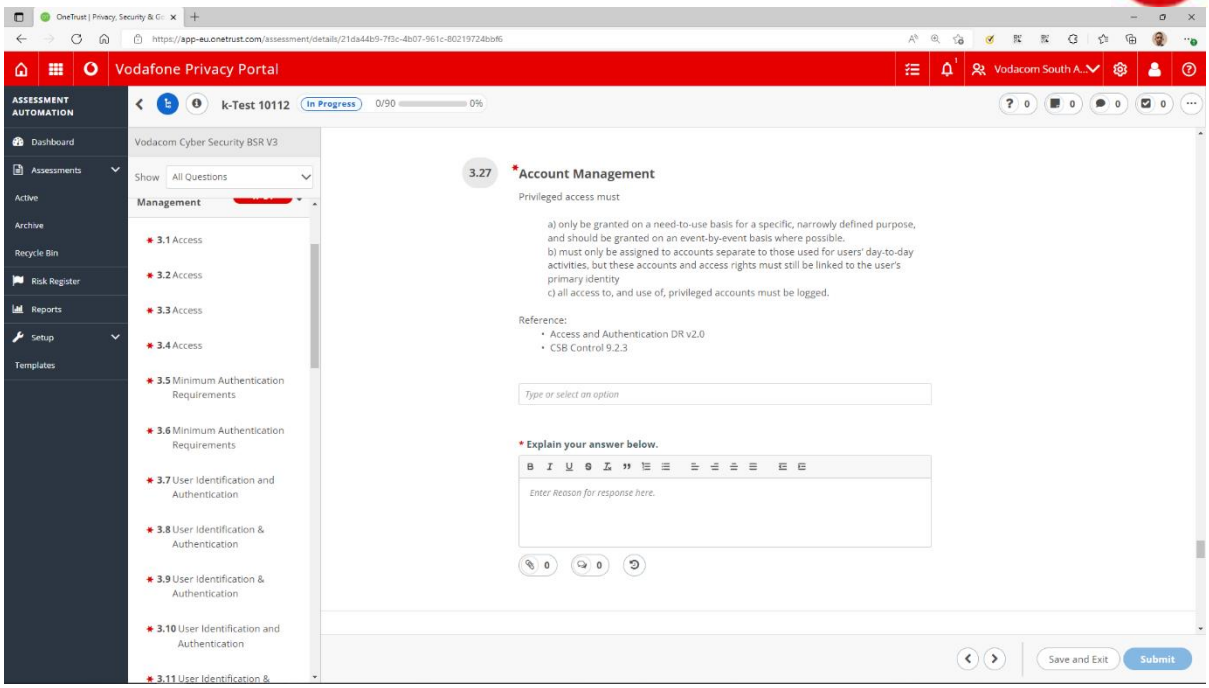


Figure 84

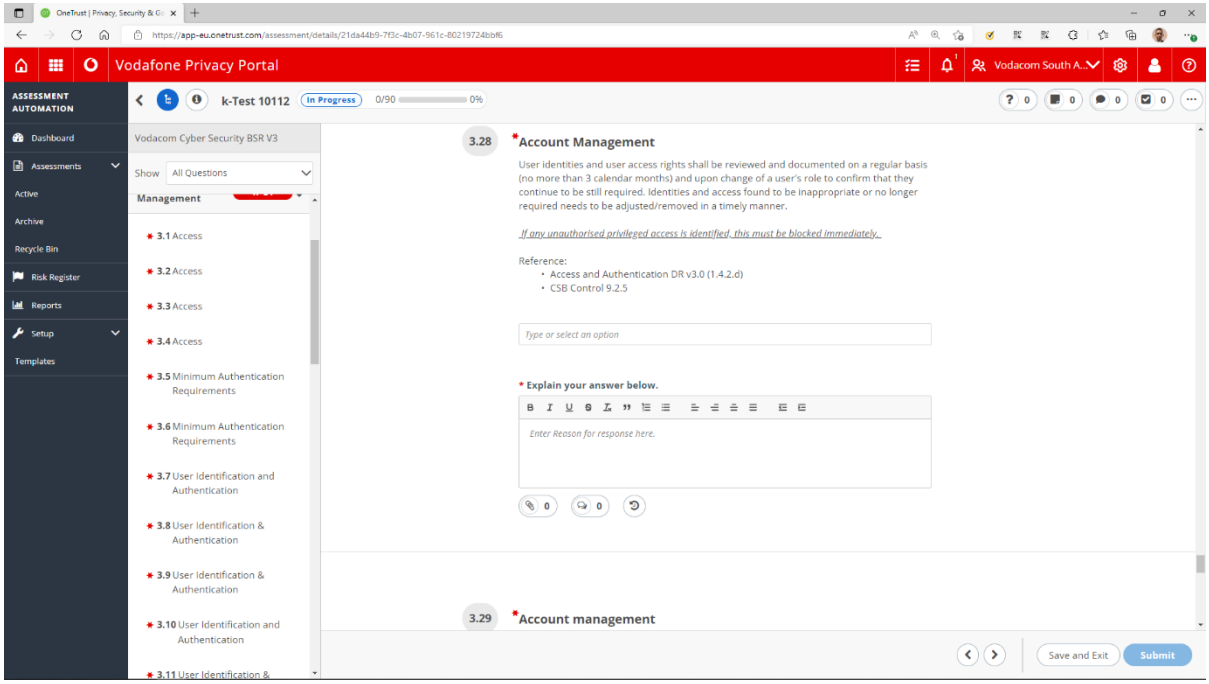


Figure 85

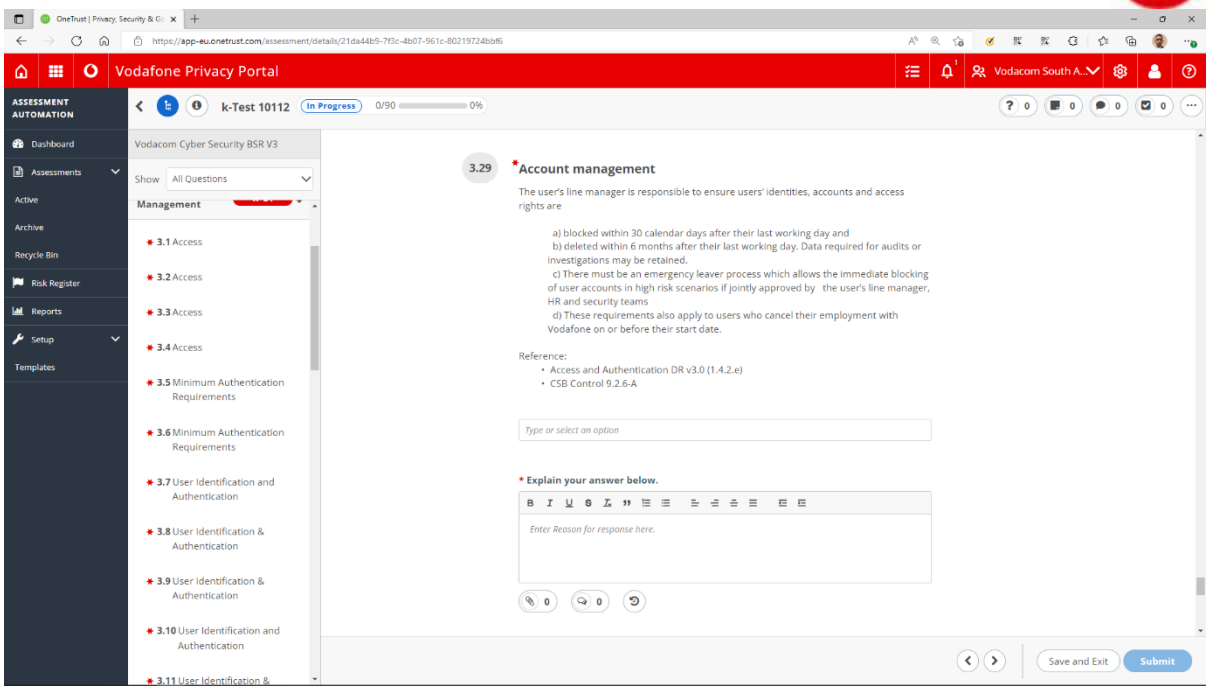


Figure 86

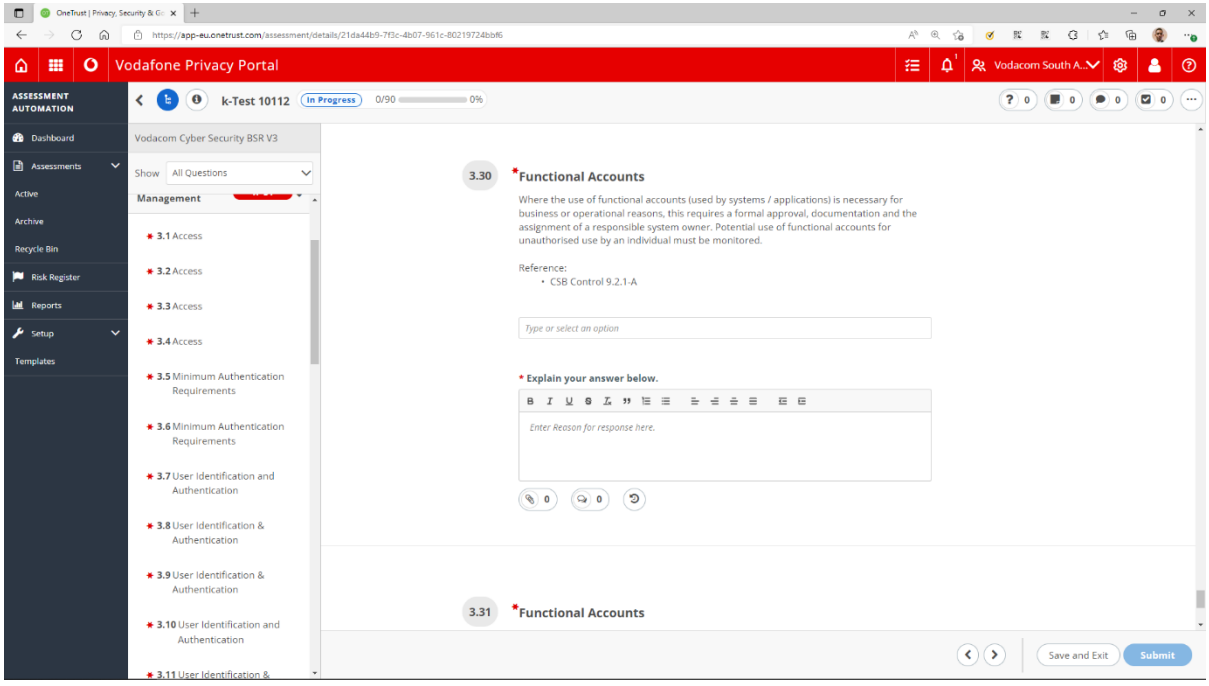


Figure 87

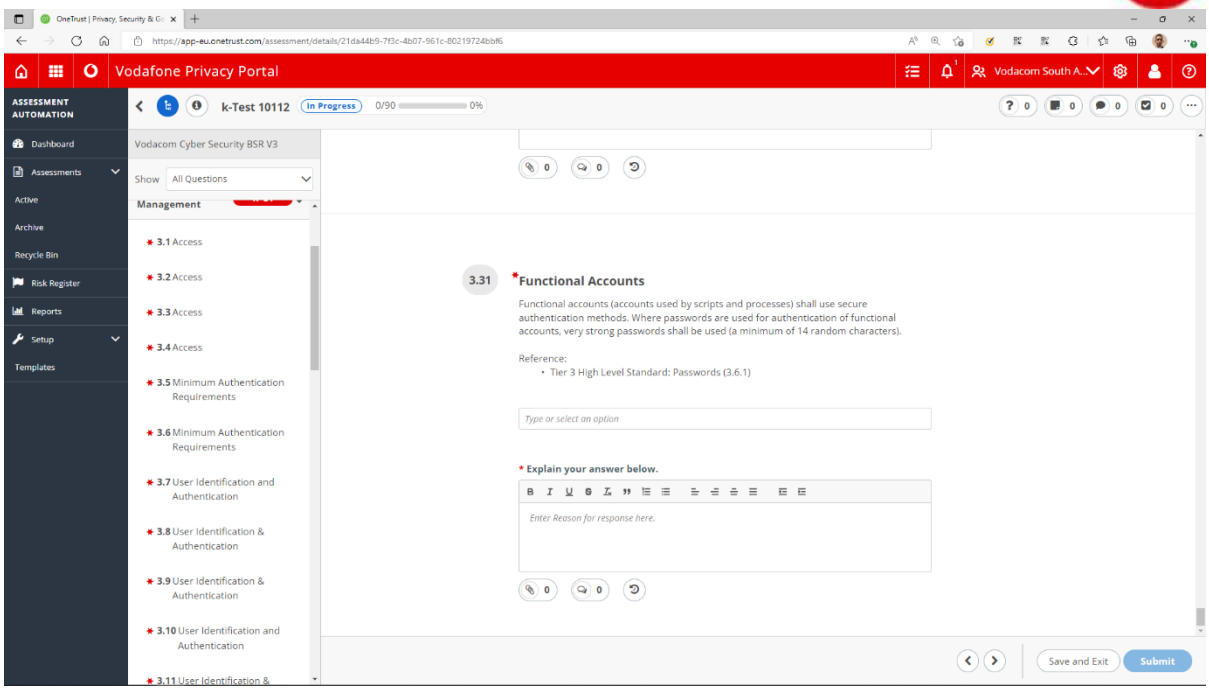

Vodafone Privacy Portal
ASSESSMENT AUTOMATION
Dashboard
Assessments
Active
Archive
Recycle Bin
Risk Register
Reports
Setup
Templates
k-Test 10112
In Progress
0/90
0%
Vodacom Cyber Security BSR V3
Show
All Questions
Management
3.1 Access
3.2 Access
3.3 Access
3.4 Access
3.5 Minimum Authentication Requirements
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 &
3.31
*Functional Accounts
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).
Reference:
• Tier 3 High Level Standard: Passwords (3.6.1)
Type or select an option
* Explain your answer below.
Enter Reason for response here.
Save and Exit
Submit

Figure 88

5.4 Data Protection

Questions 4.1 to 4.4

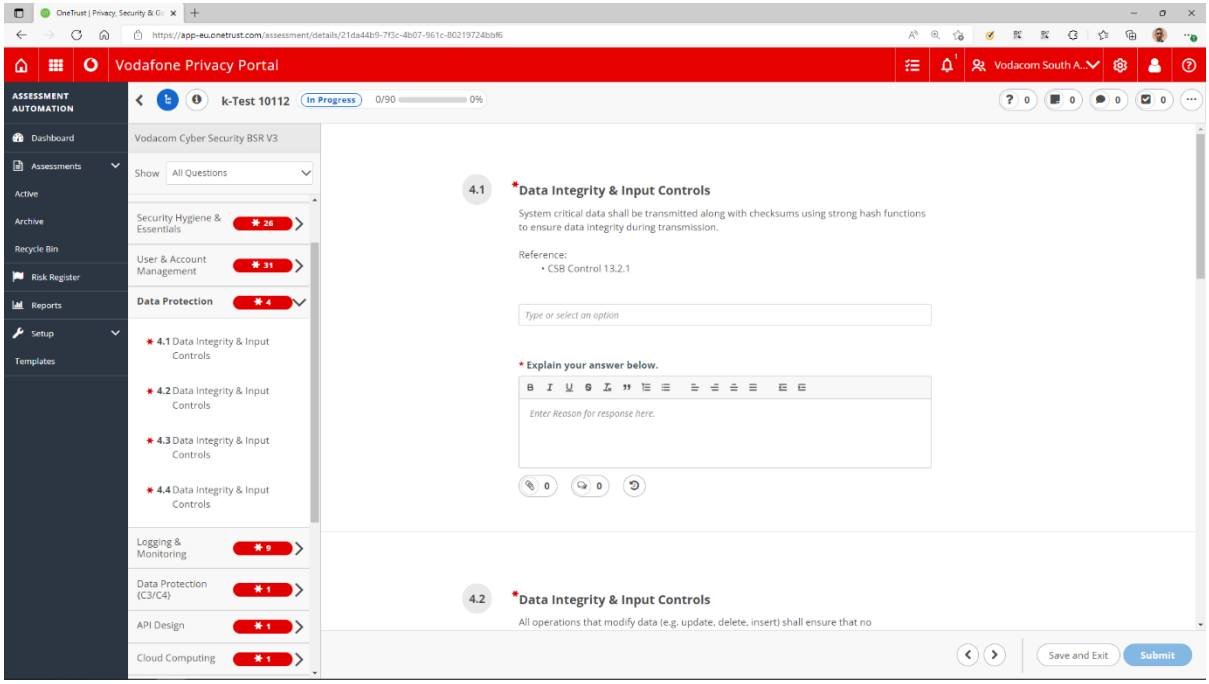


Figure 89

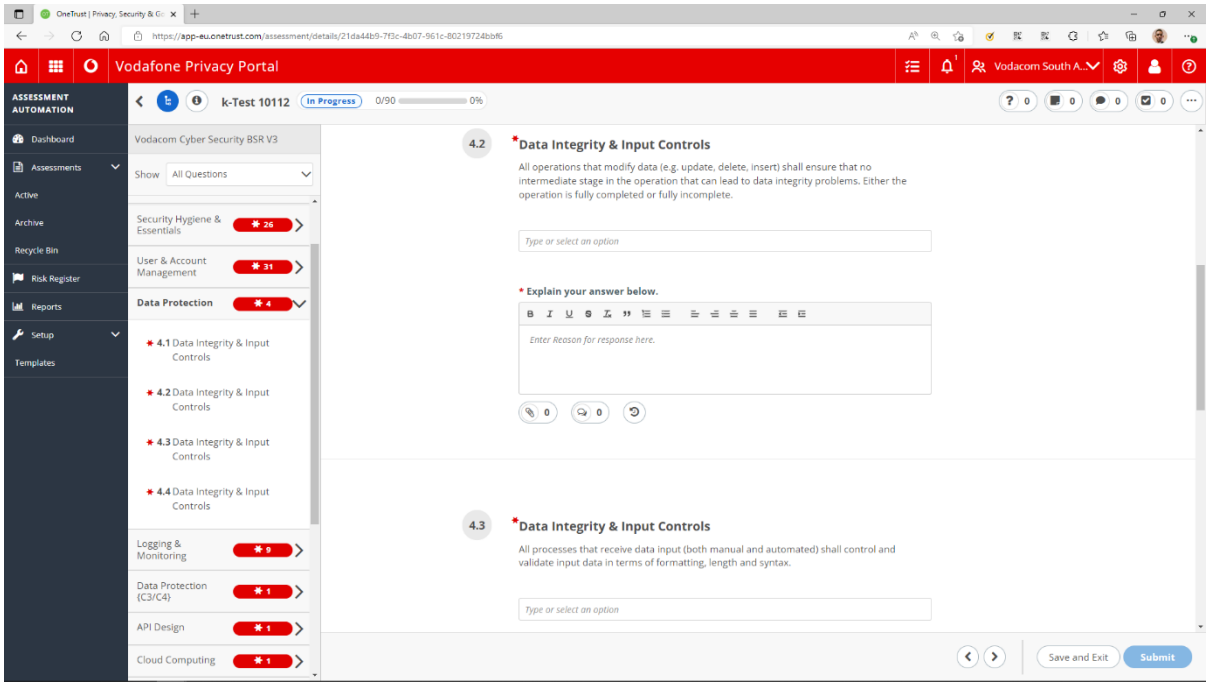


Figure 90

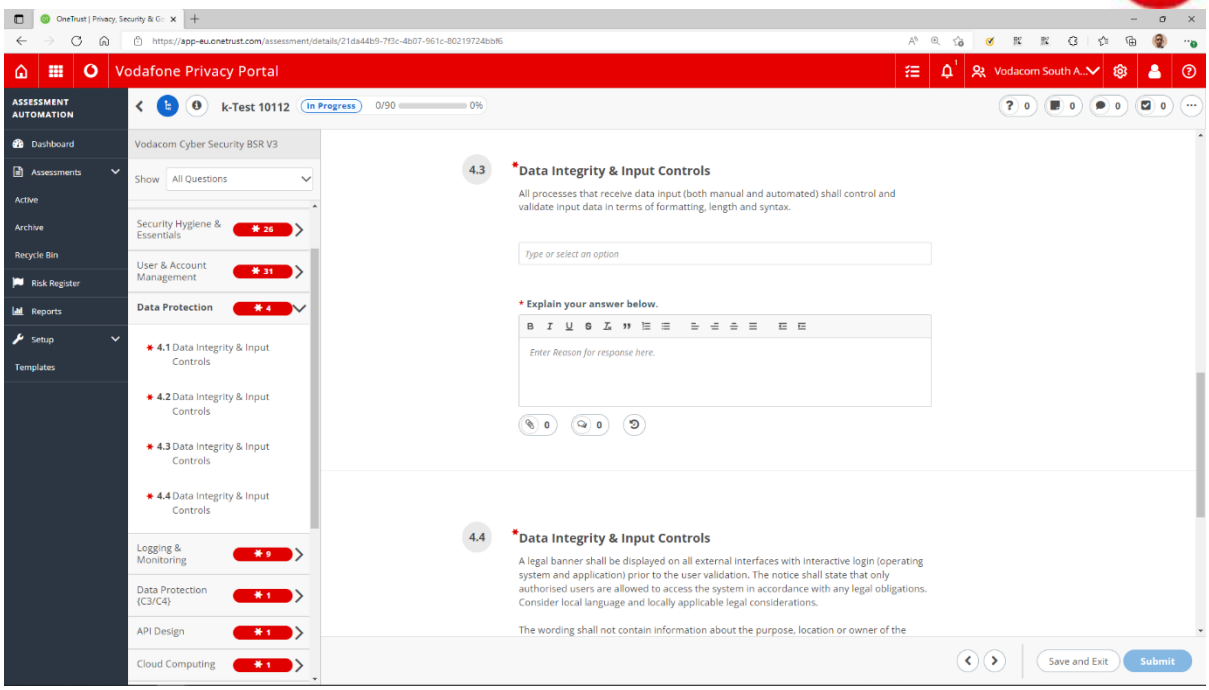


Figure 91

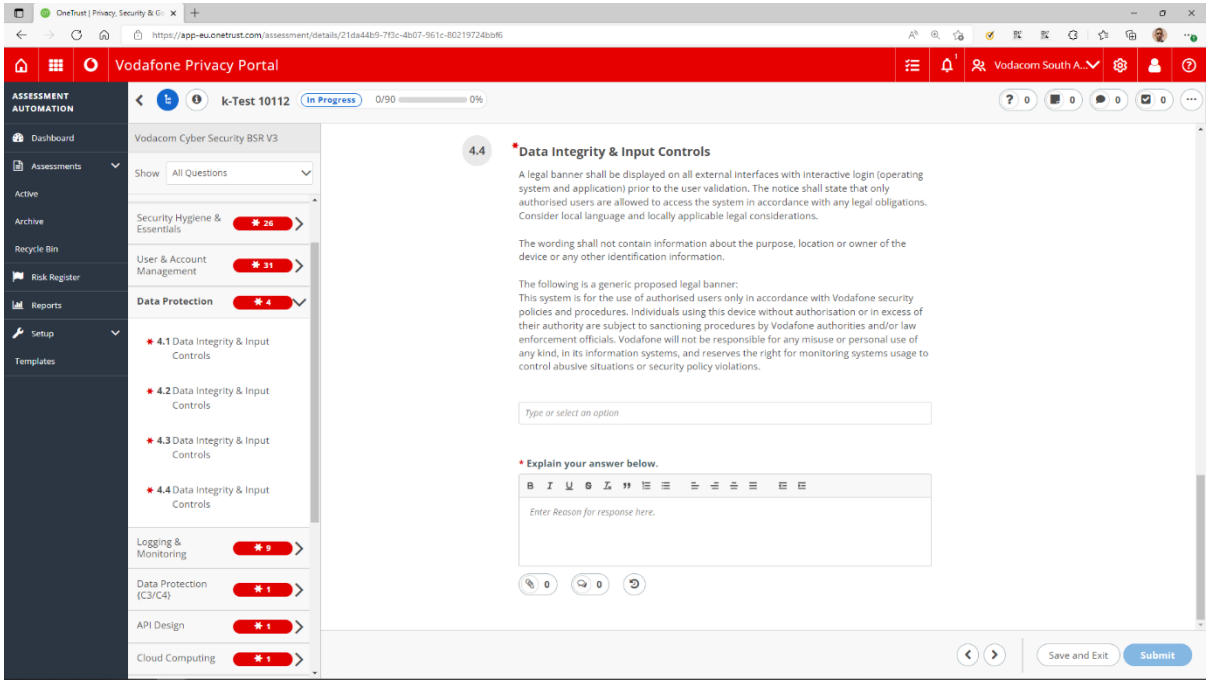


Figure 92

5.5 Logging and Monitoring

Questions 5.1 to 5.9

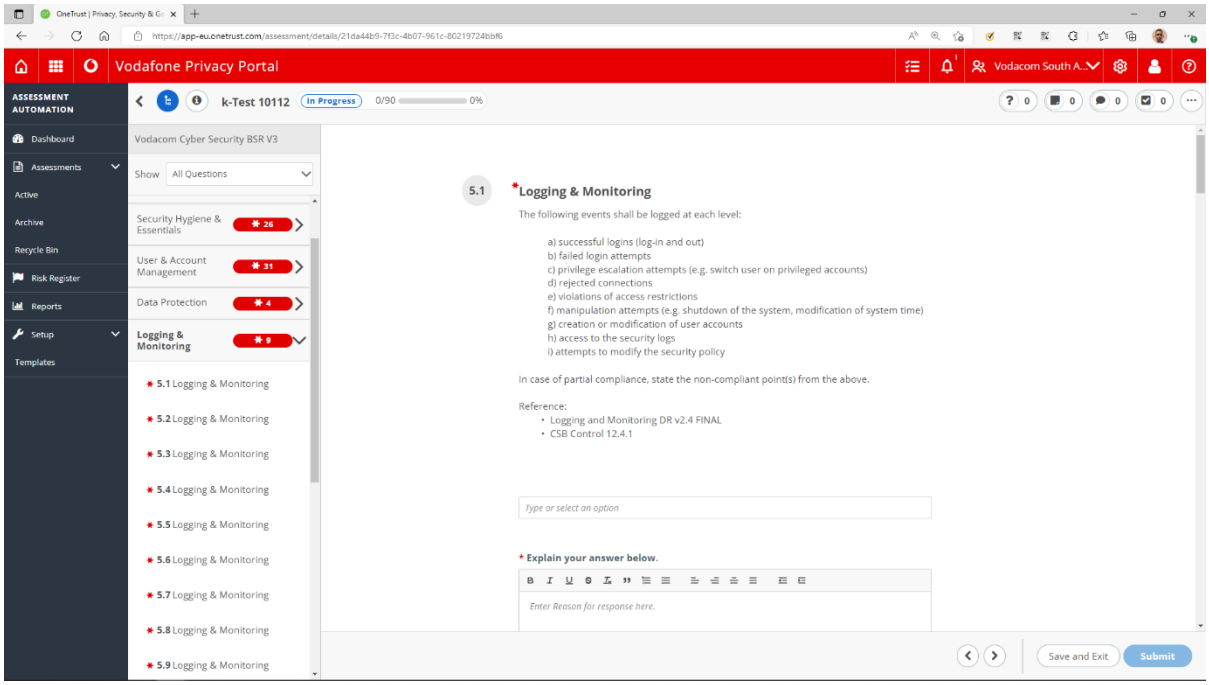


Figure 93

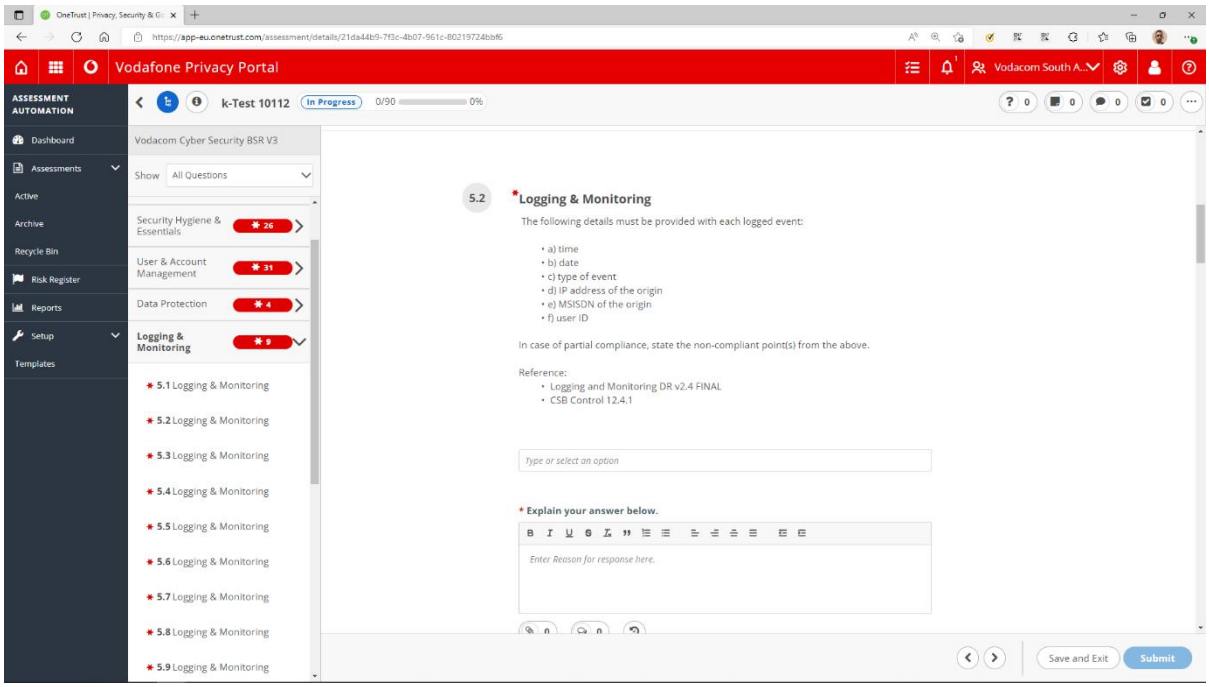


Figure 94

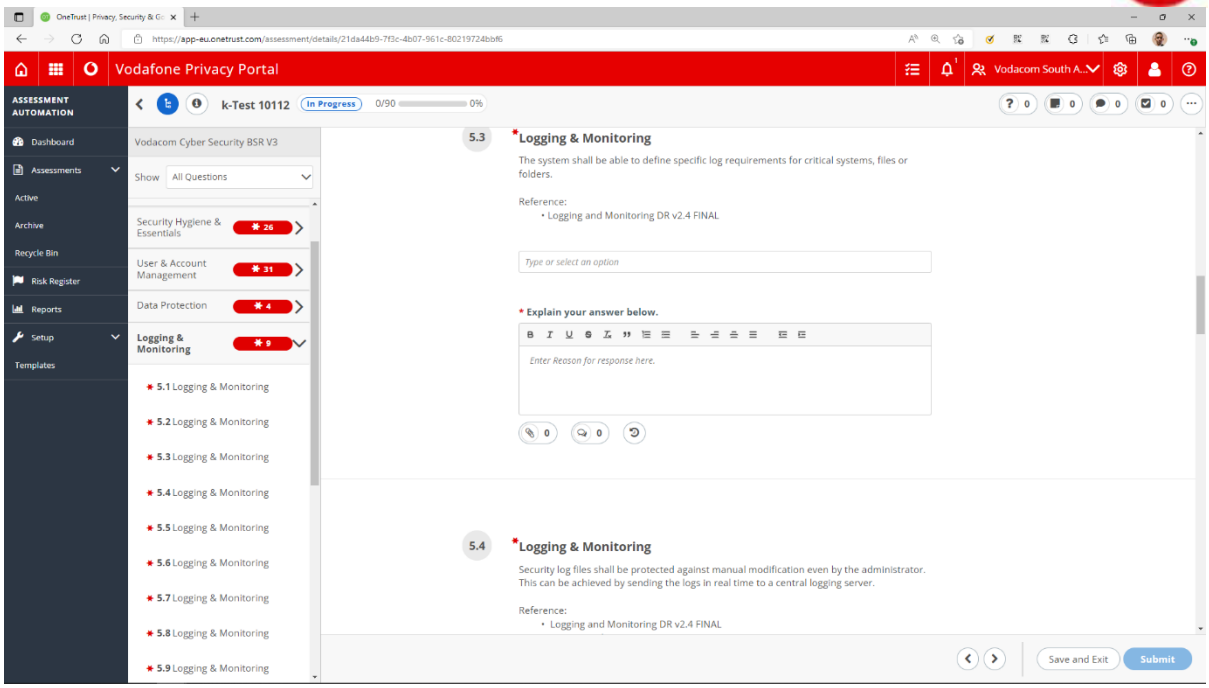


Figure 95

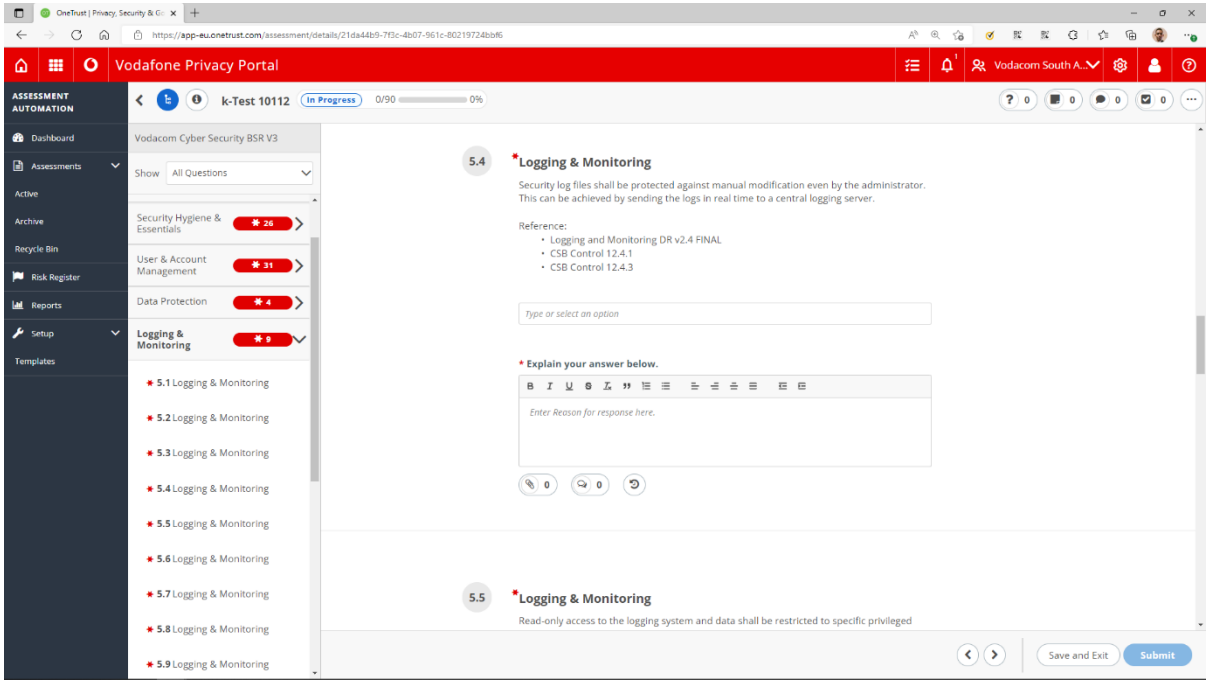


Figure 96

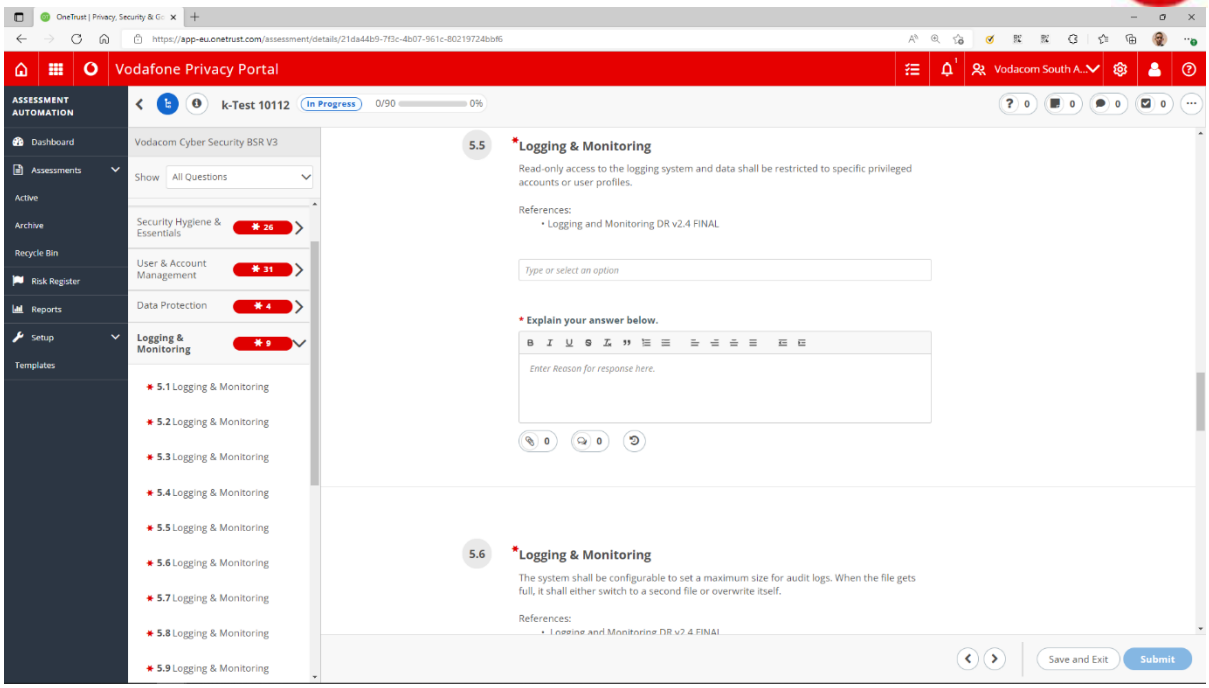


Figure 97

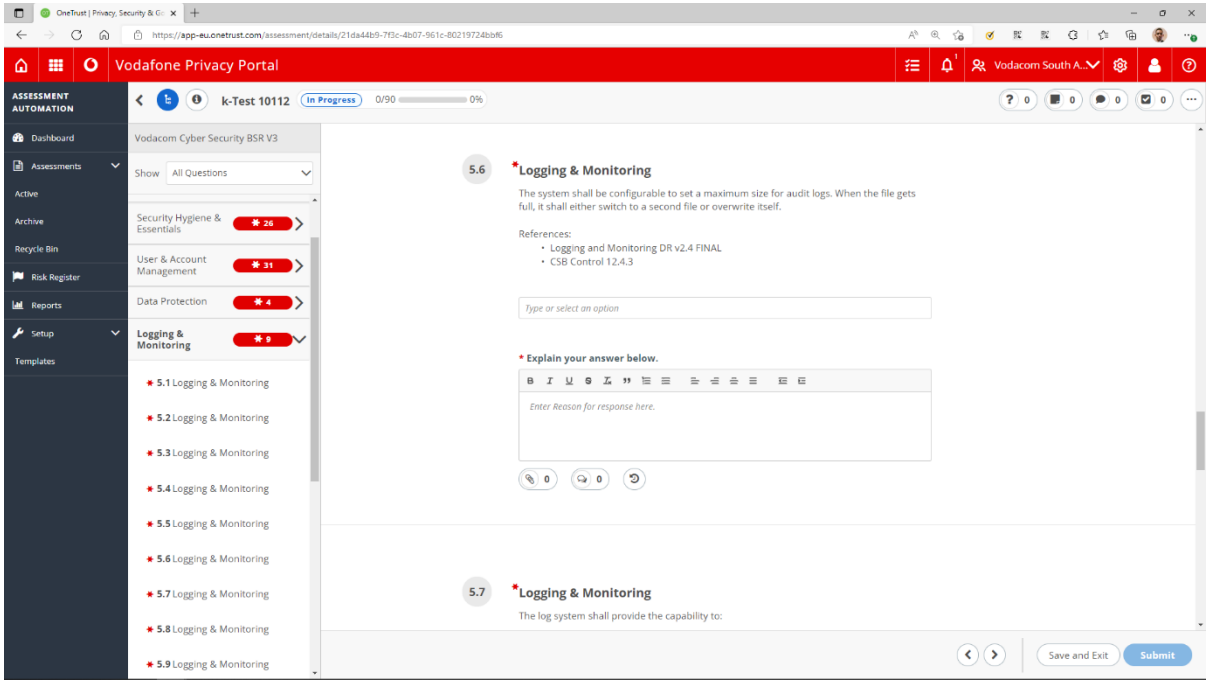


Figure 98

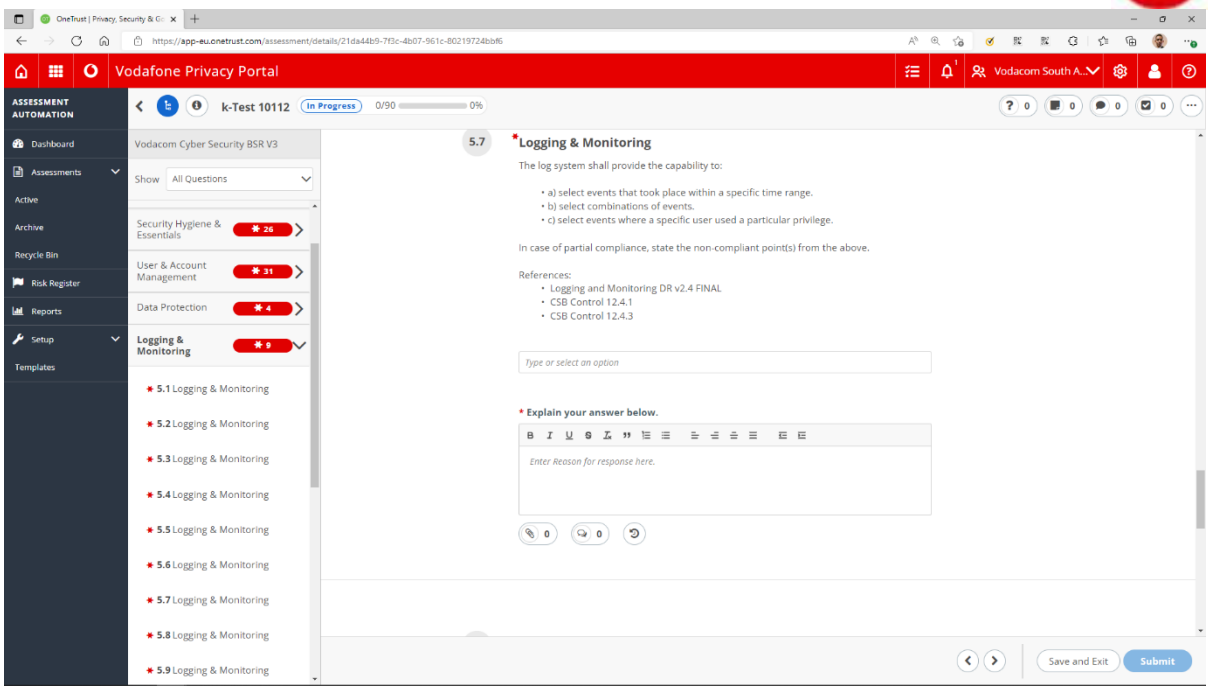


Figure 99

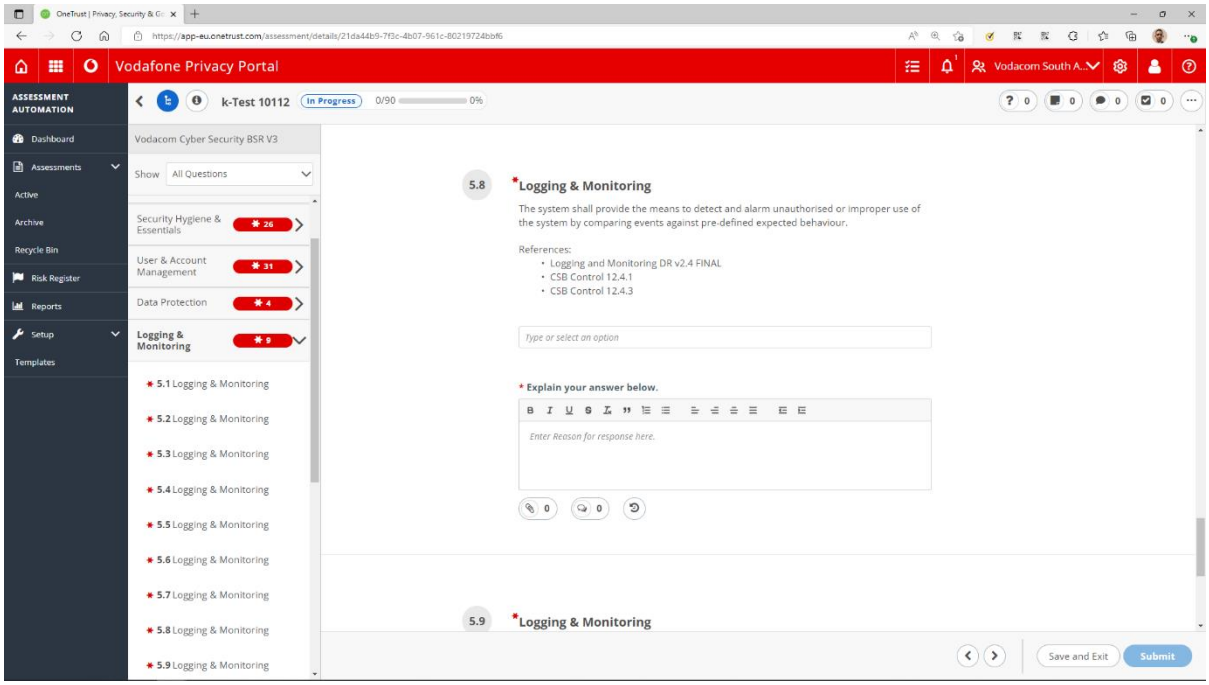


Figure 100

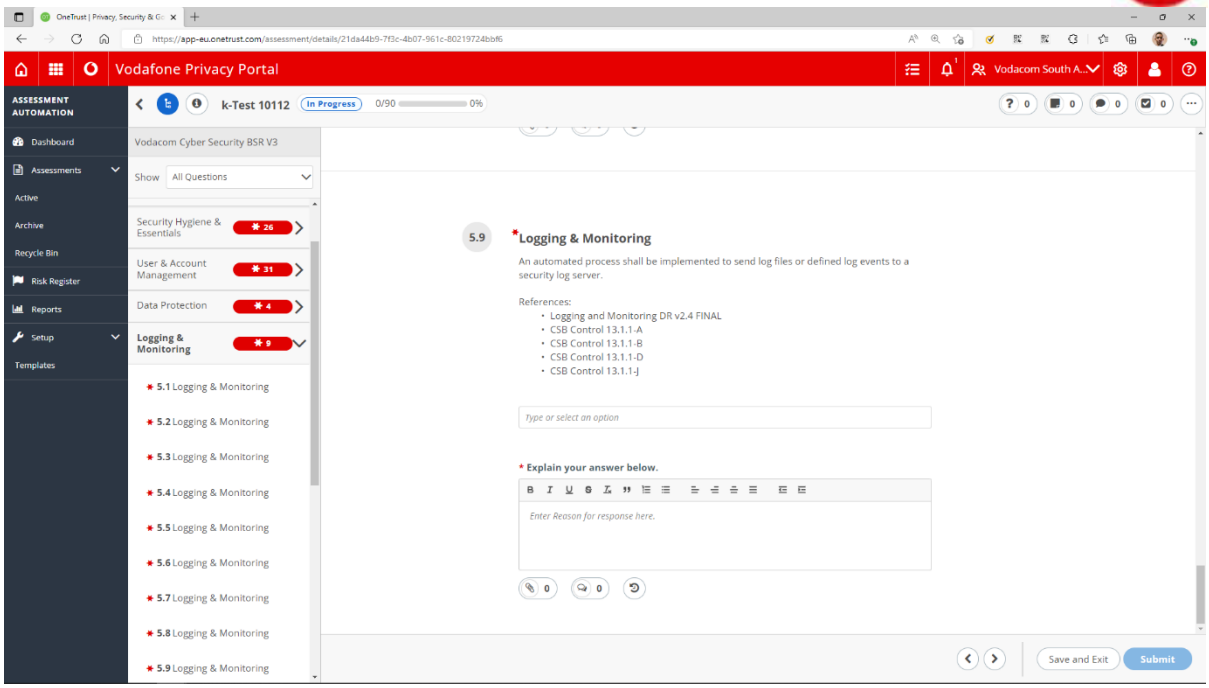

Vodafone Privacy Portal
ASSESSMENT AUTOMATION
Dashboard
Assessments
Active
Archive
Recycle Bin
Risk Register
Reports
Setup
Templates
k-Test 10112
In Progress
0/90
0%
Vodacom Cyber Security BSR V3
Show
All Questions
Security Hygiene & Essentials
26
User & Account Management
31
Data Protection
4
Logging & Monitoring
9
5.1 Logging & Monitoring
5.2 Logging & Monitoring
5.3 Logging & Monitoring
5.4 Logging & Monitoring
5.5 Logging & Monitoring
5.6 Logging & Monitoring
5.7 Logging & Monitoring
5.8 Logging & Monitoring
5.9 Logging & Monitoring
5.9
Logging & Monitoring
An automated process shall be implemented to send log files or defined log events to a security log server.
References:
Logging and Monitoring DR v2.4 FINAL
CSB Control 13.1.1-A
CSB Control 13.1.1-B
CSB Control 13.1.1-D
CSB Control 13.1.1-J
Type or select an option
Explain your answer below.
Enter Reason for response here.
Save and Exit
Submit

Figure 101

5.6 Data Protection {C3/C4}

Question 6.1

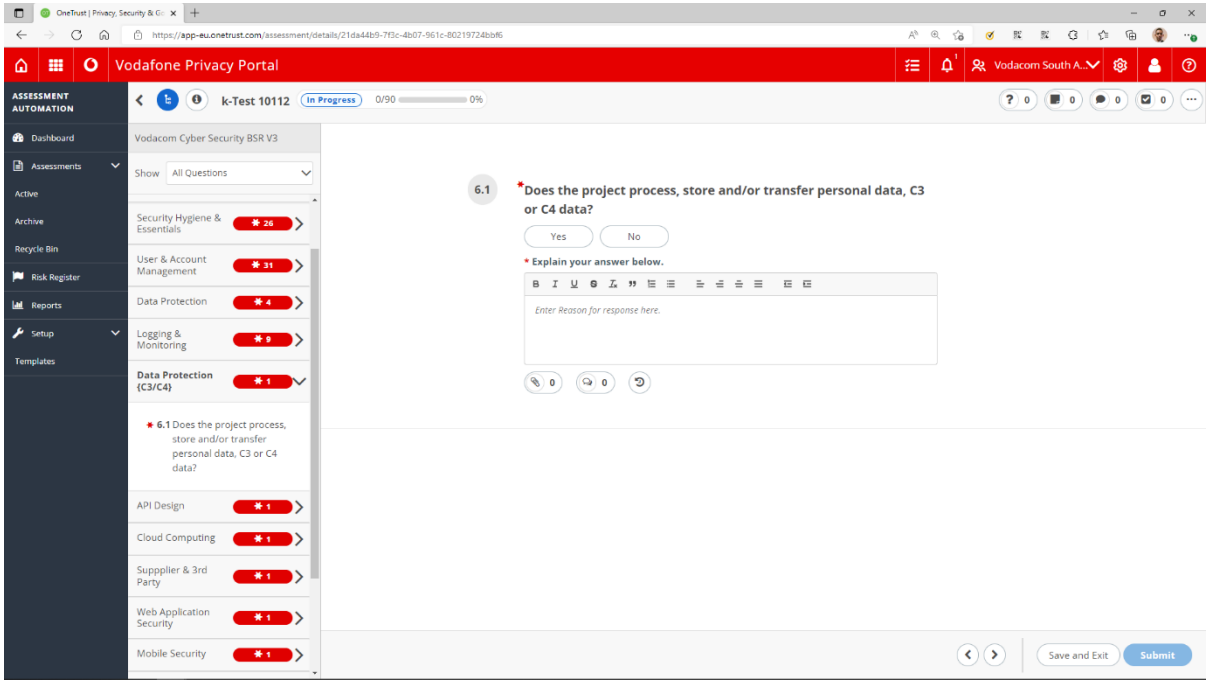


Figure 102

5.7 API Design

Question 7.1

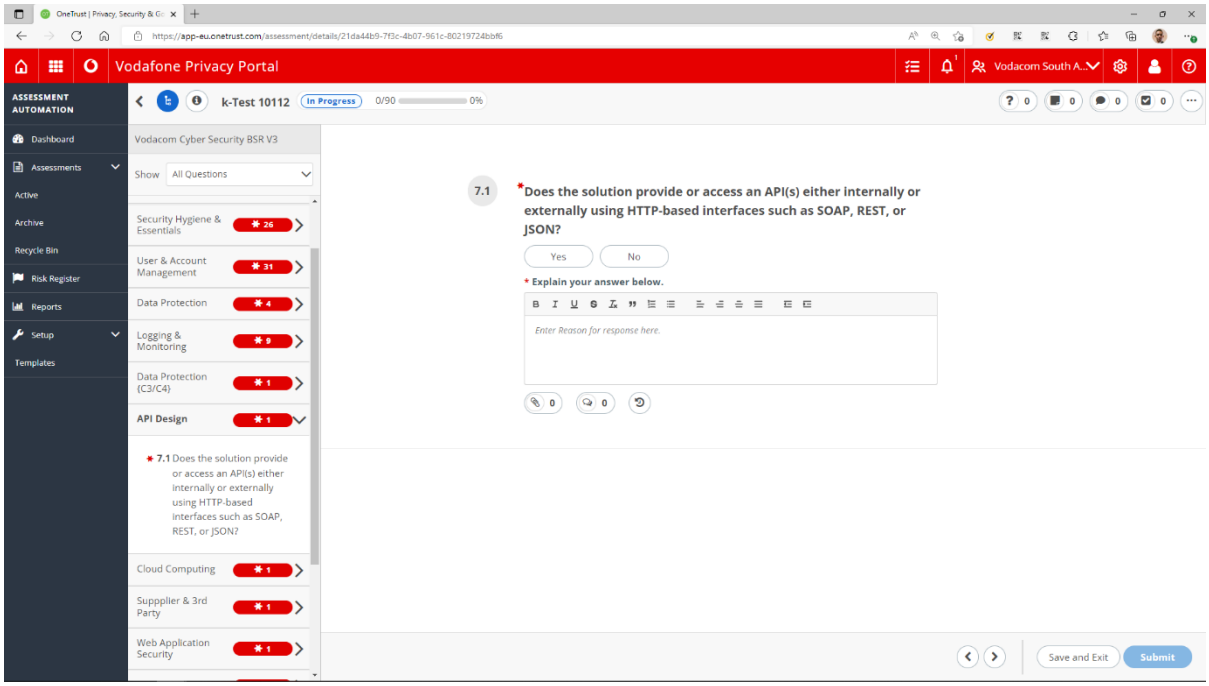


Figure 103

5.8 Cloud Computing

Question 8.1

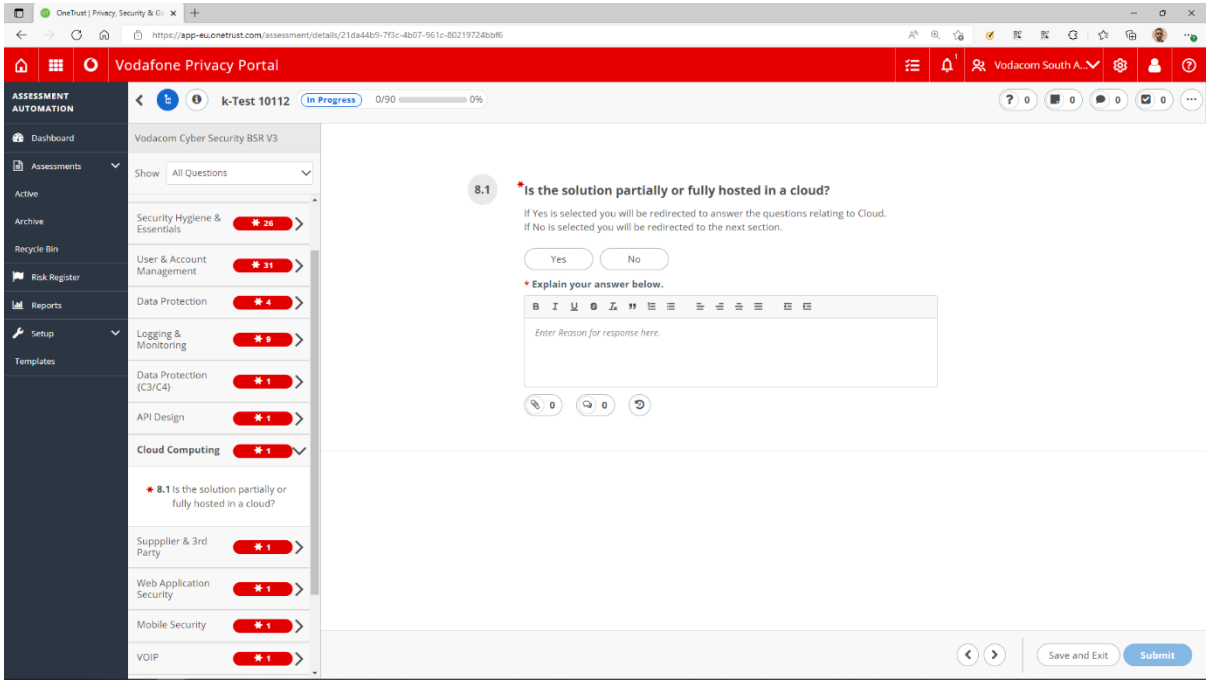


Figure 104

5.9 Web Application

Question 9.1

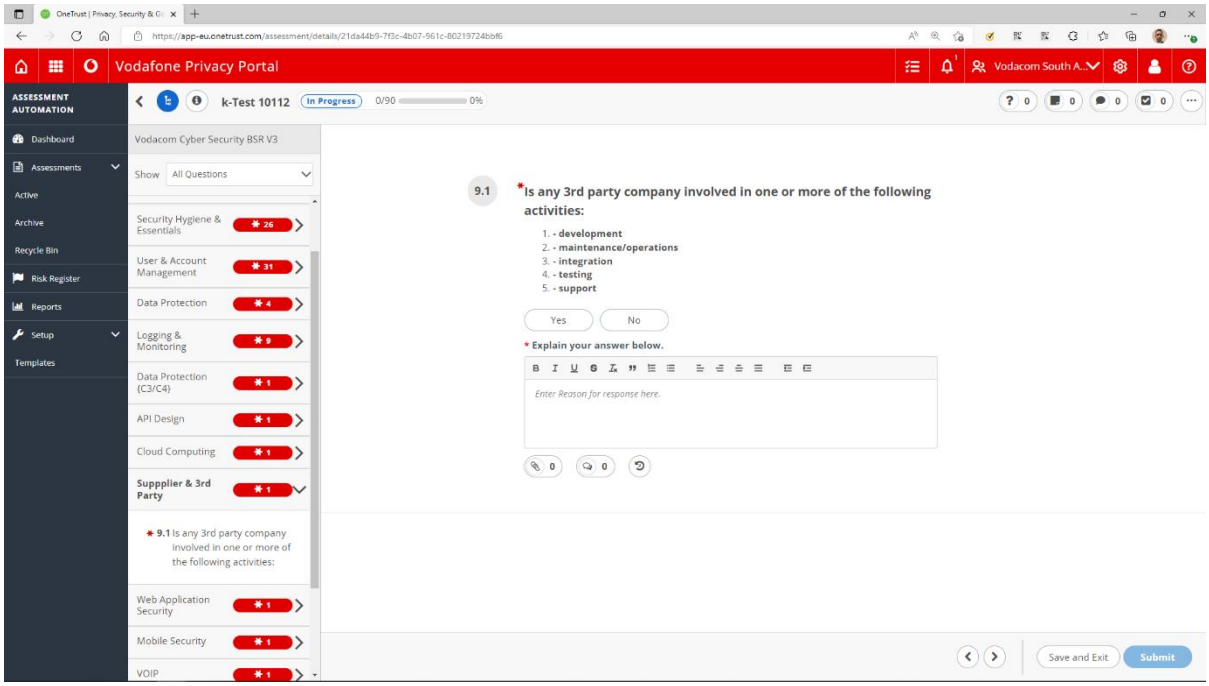


Figure 105

5.10 Web Application Security

Question 10.1

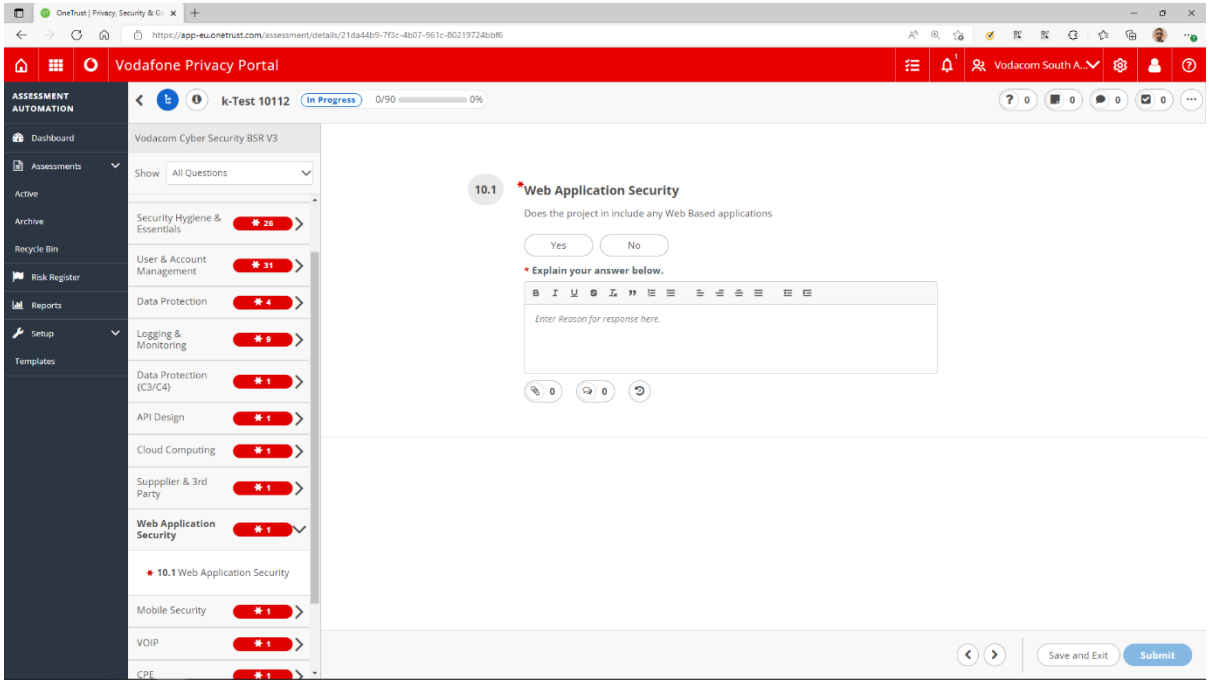


Figure 106

5.11 Mobile Security

Question 11.1

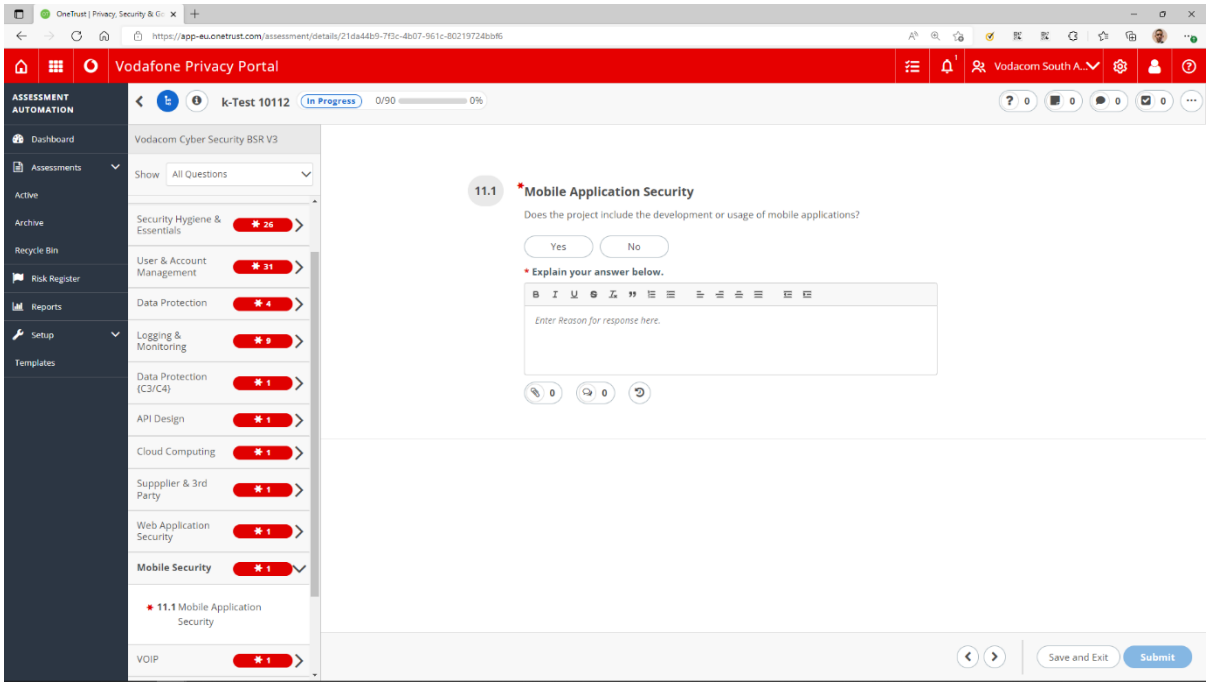


Figure 107

5.12 Monitoring & Logging

Question 12.1

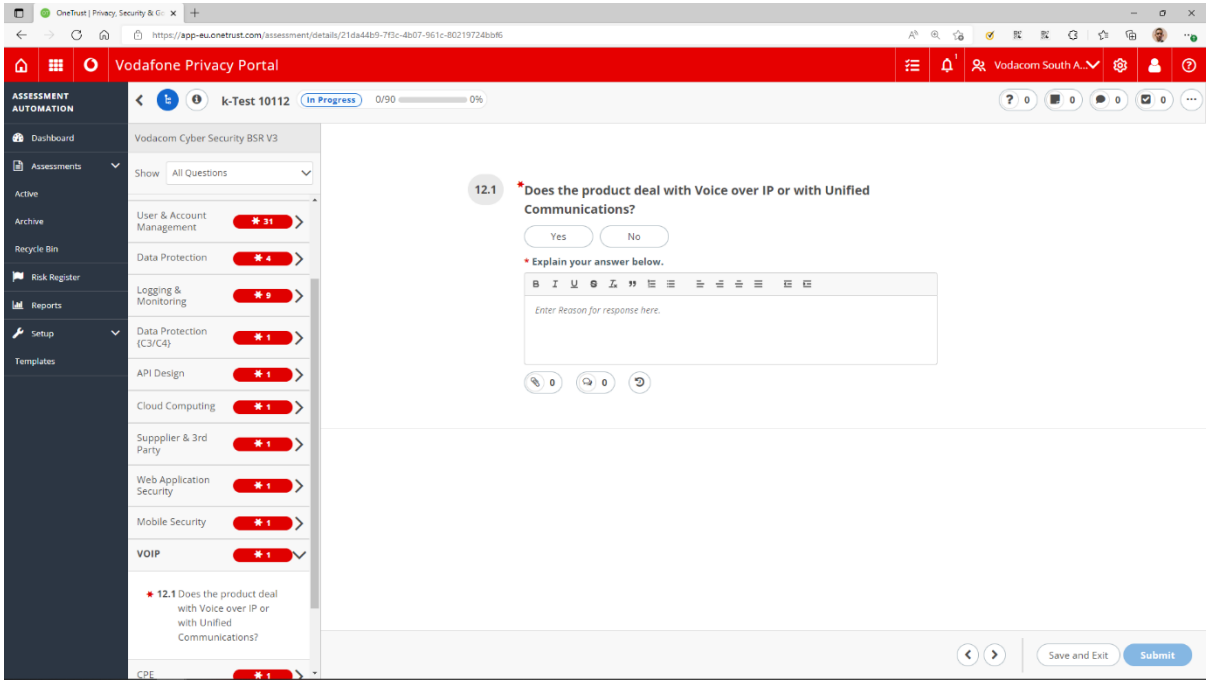


Figure 108

5.13 CPE

Question 13.1

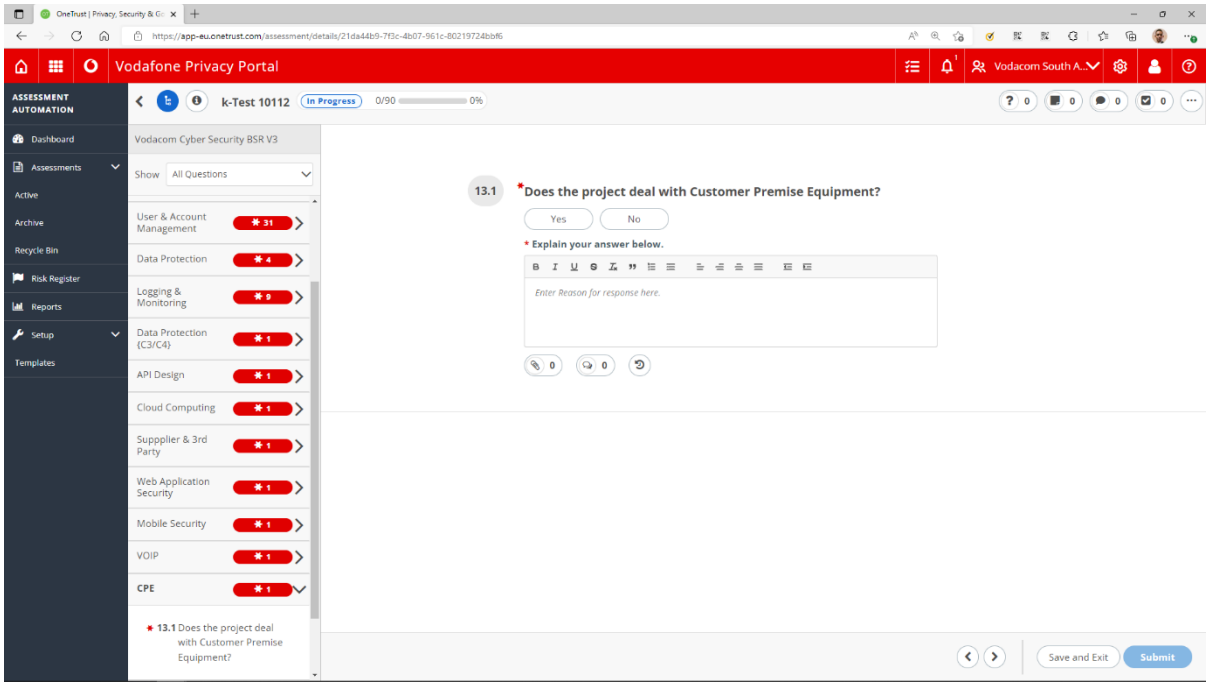


Figure 109

5.14 Technical Assurance

Question 14.1 to 14.2

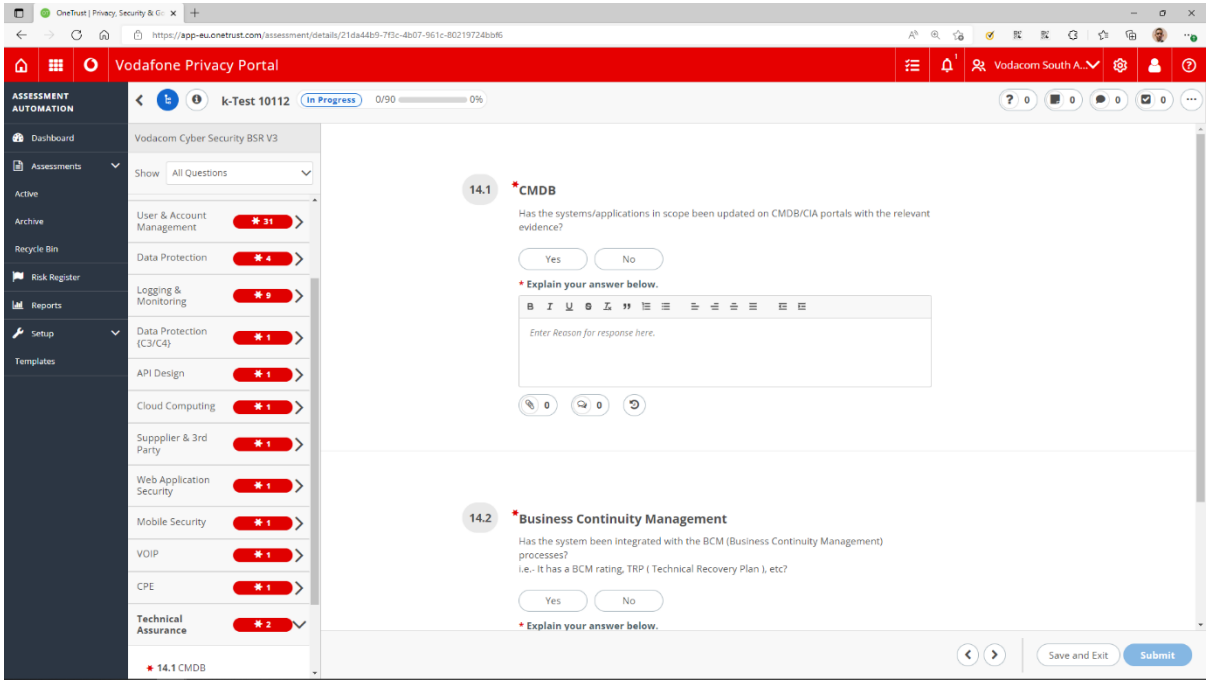


Figure 110

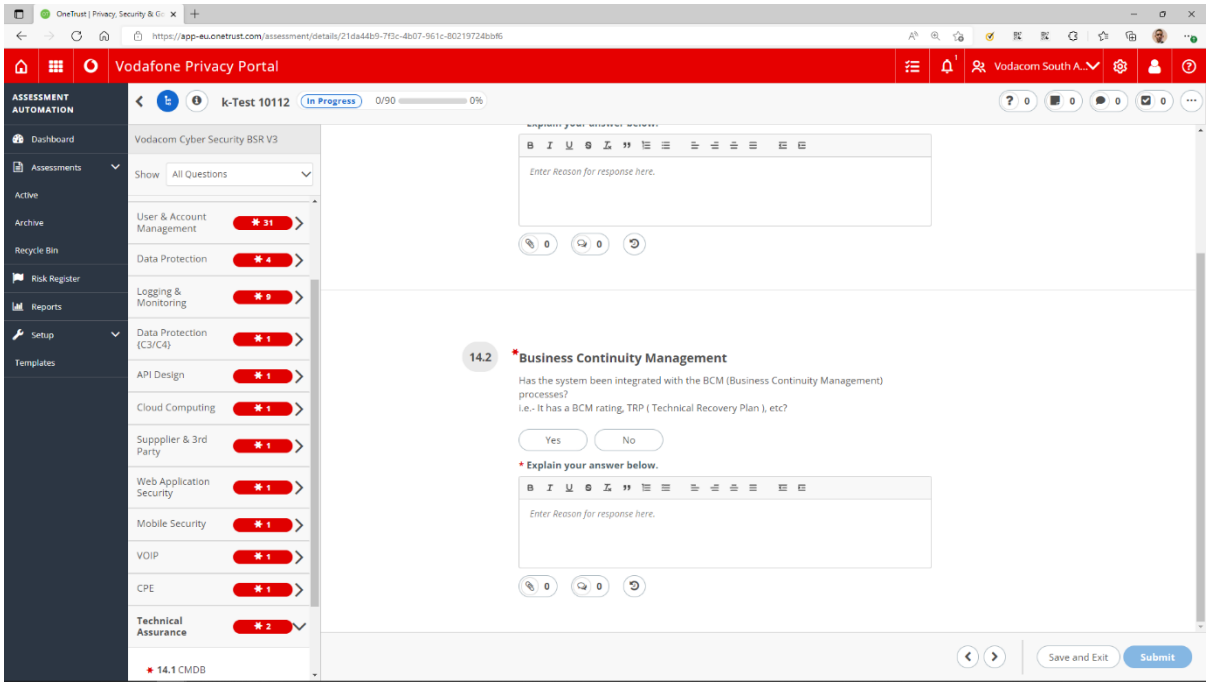


Figure 111

5.15 End of Assessment

Question 15.1

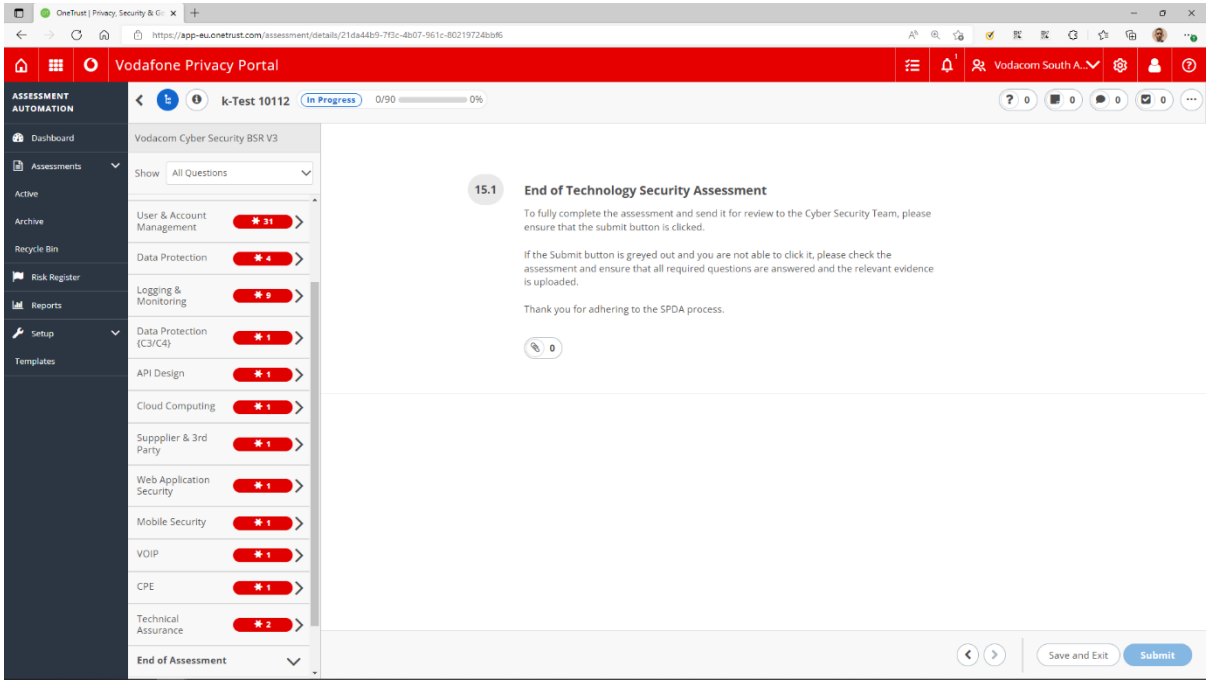


Figure 112

6. OneTrust: How to Raise a Risk

Click on the Risk Register in the panel on the left

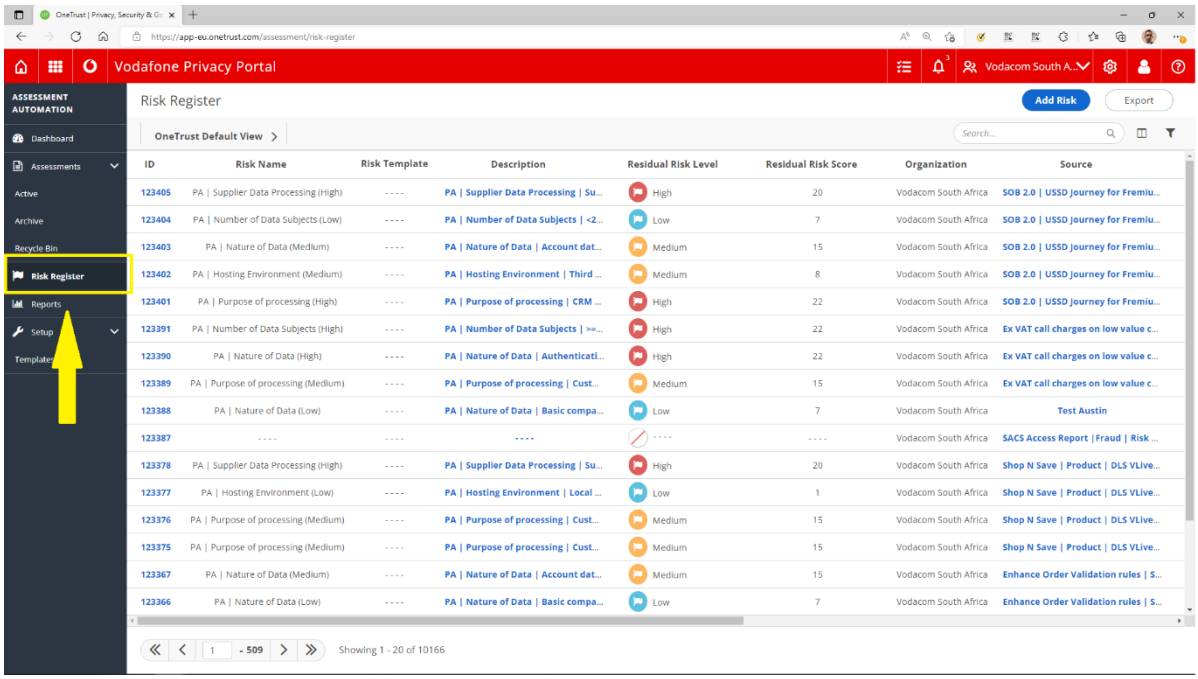


Figure 113

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

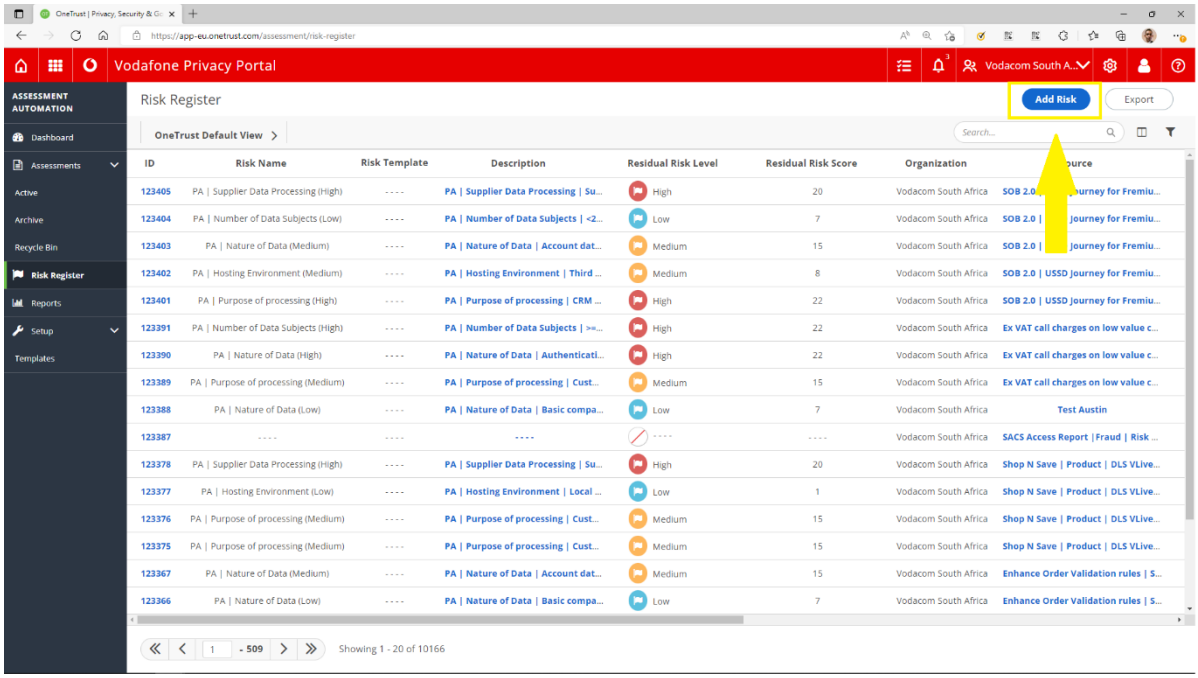


Figure 114

The CSO select the ‘Create New Risk’ radial button

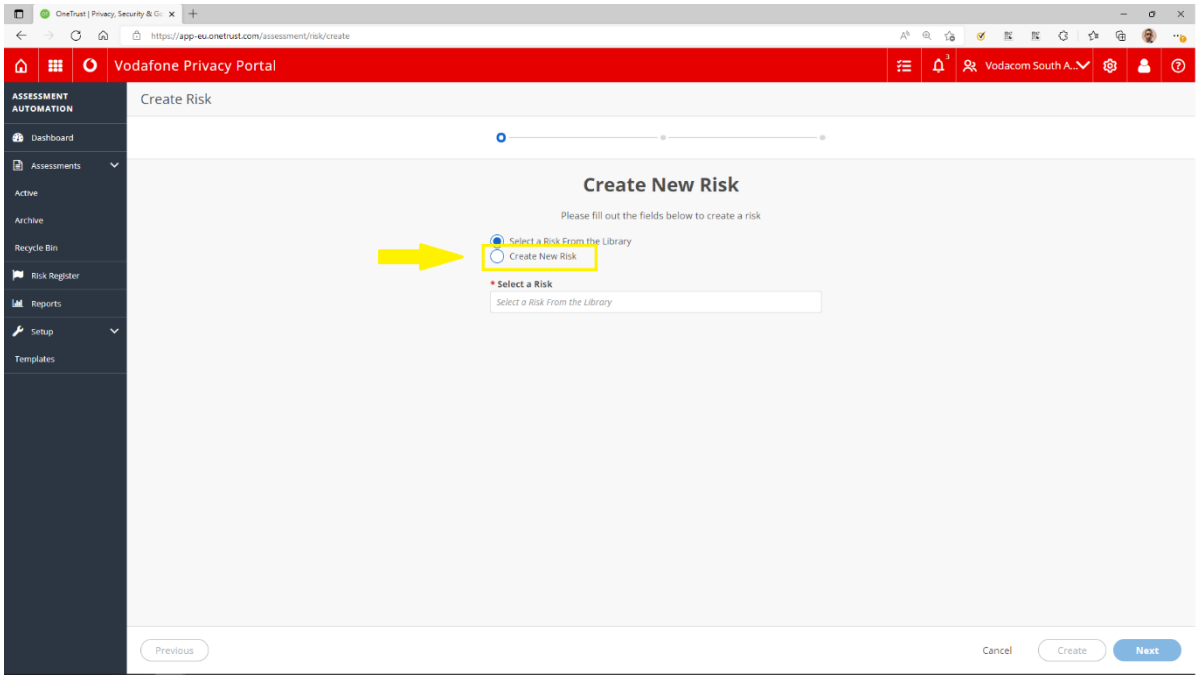


Figure 115

The ‘Create New Risk’ box will be displayed

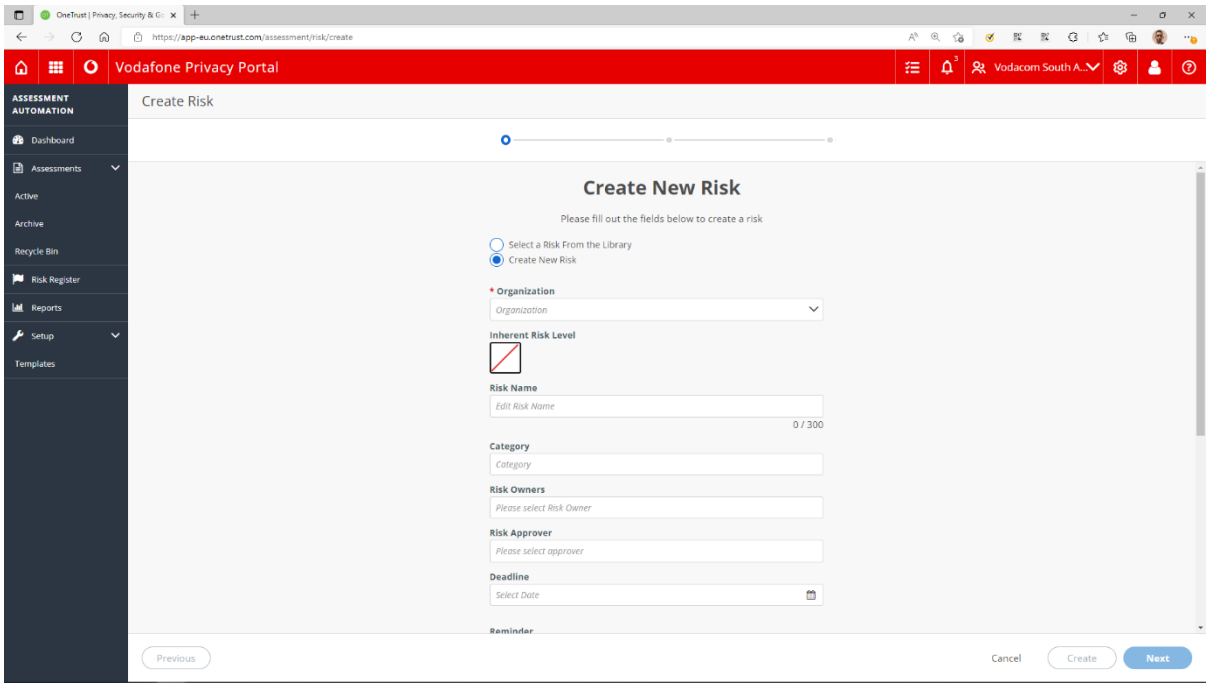


Figure 116

The CSO will then have to complete the fields raised

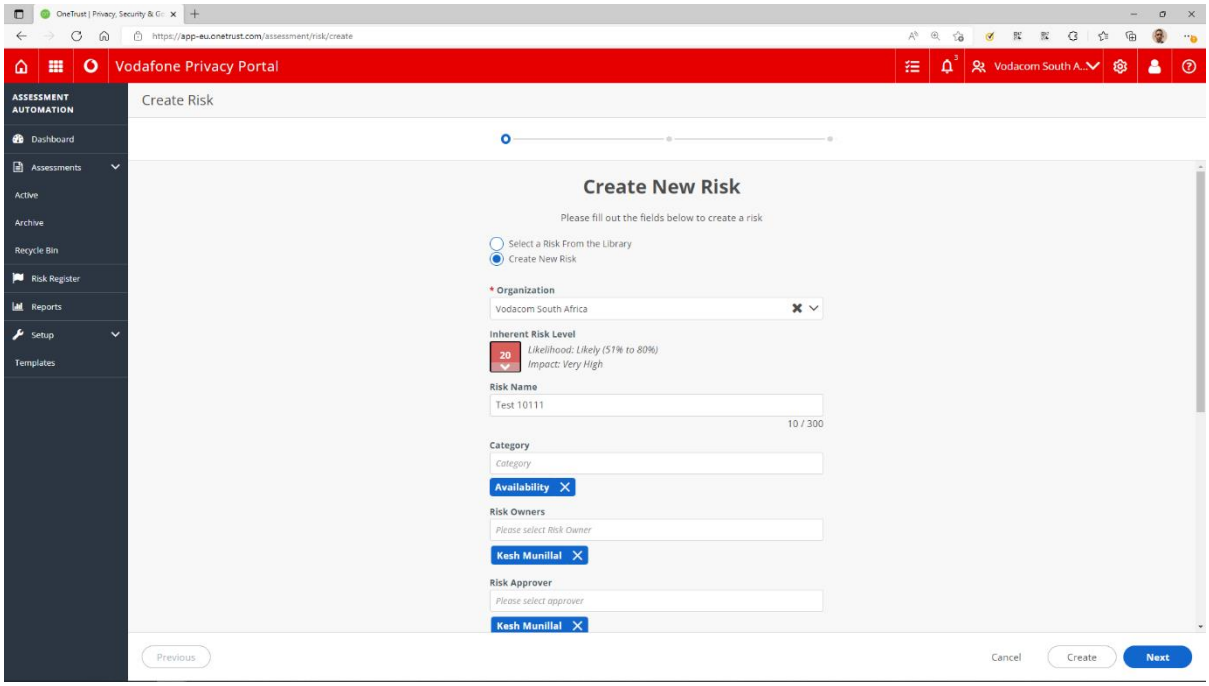


Figure 117

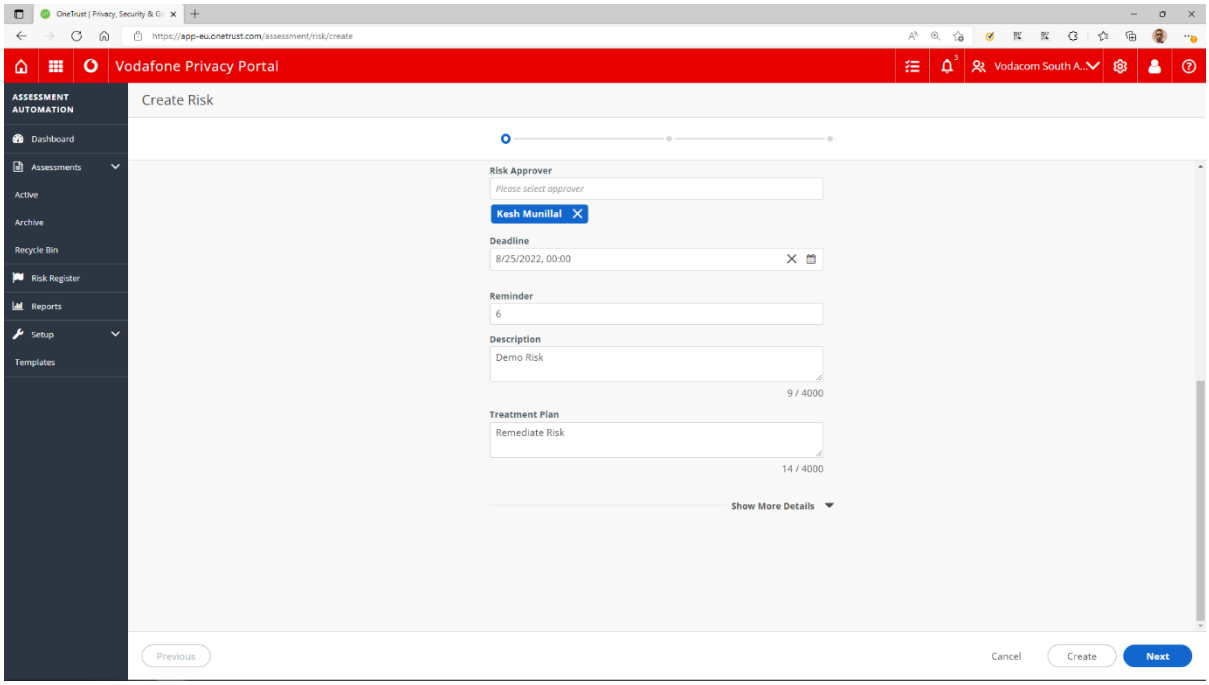


Figure 118

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

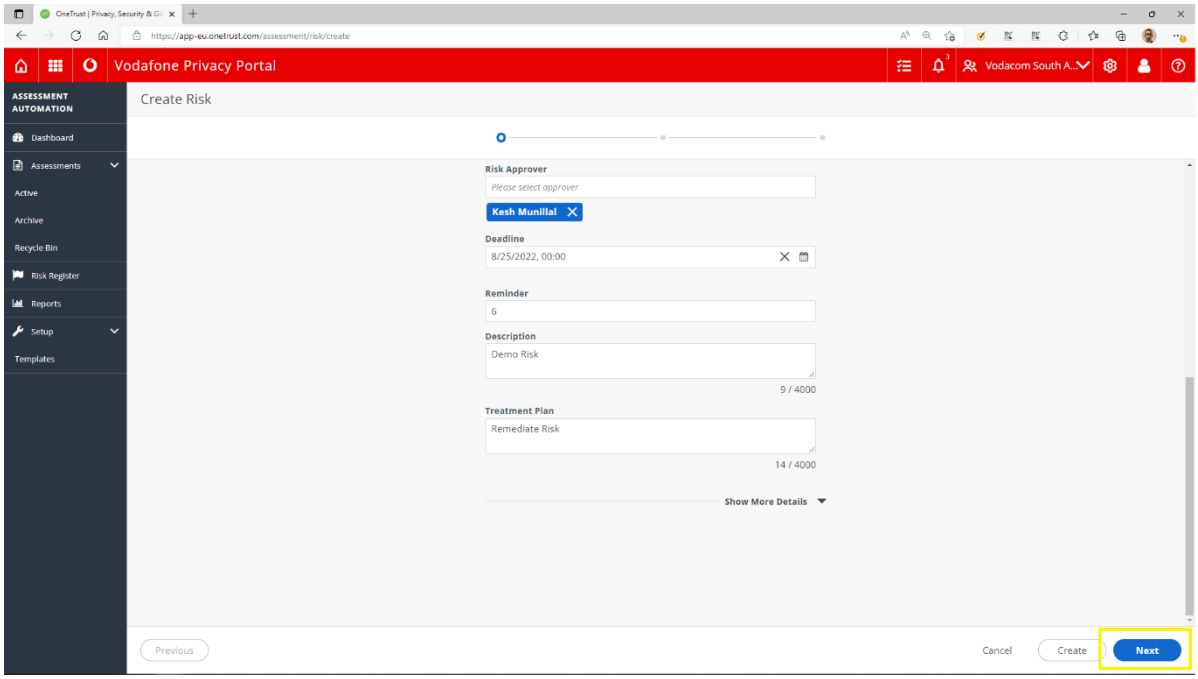


Figure 119

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

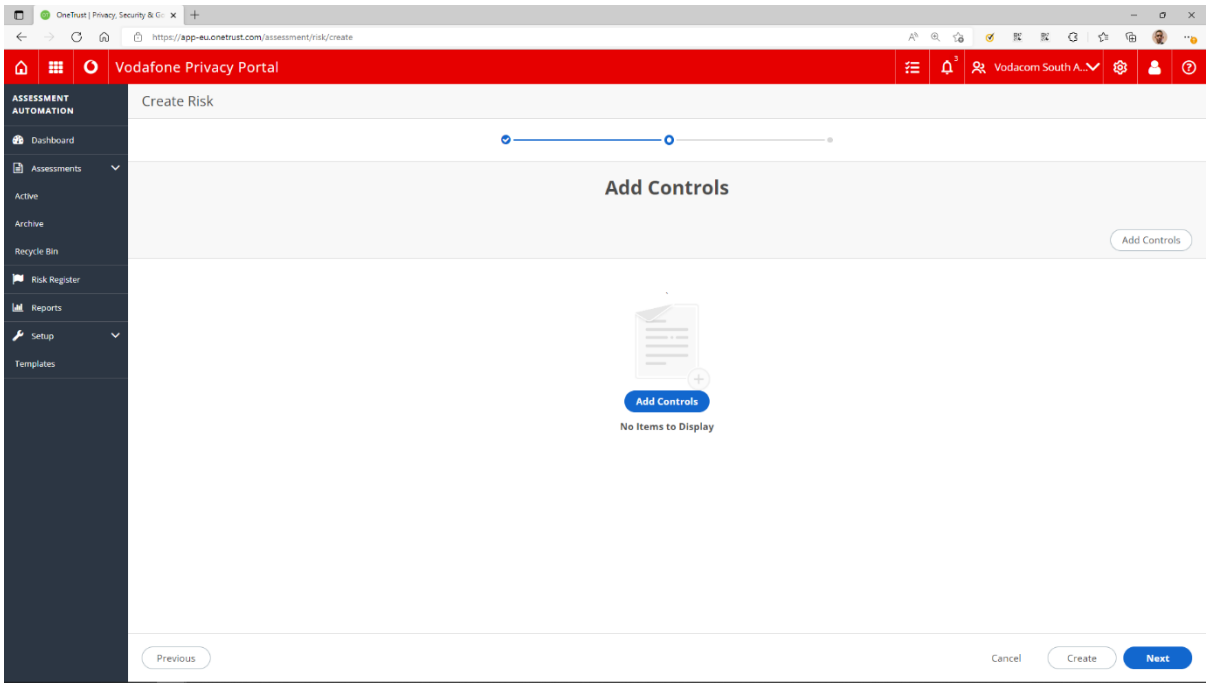


Figure 120

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

The 'Add Control' box will be displayed

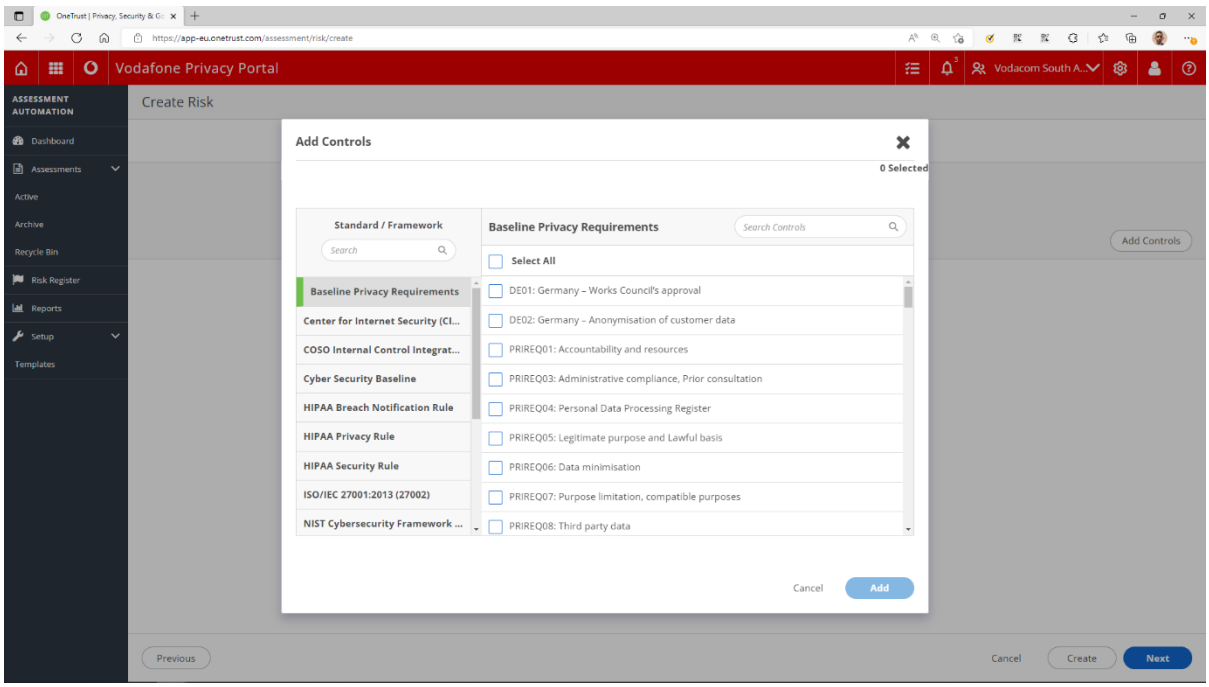


Figure 121

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

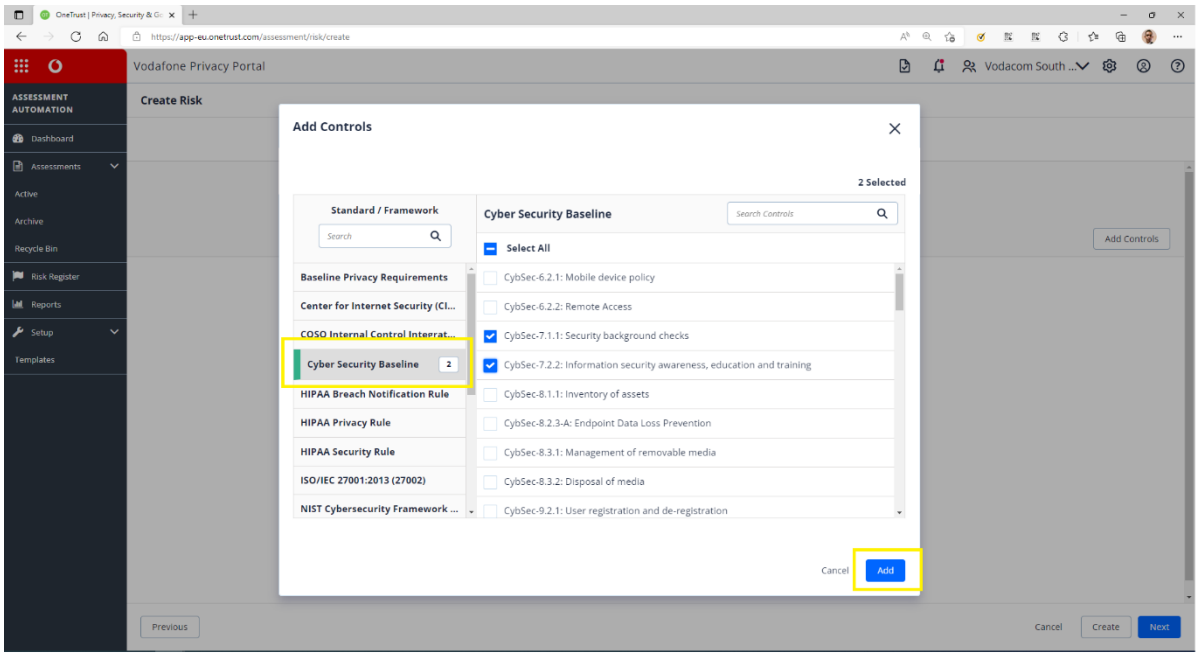


Figure122

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

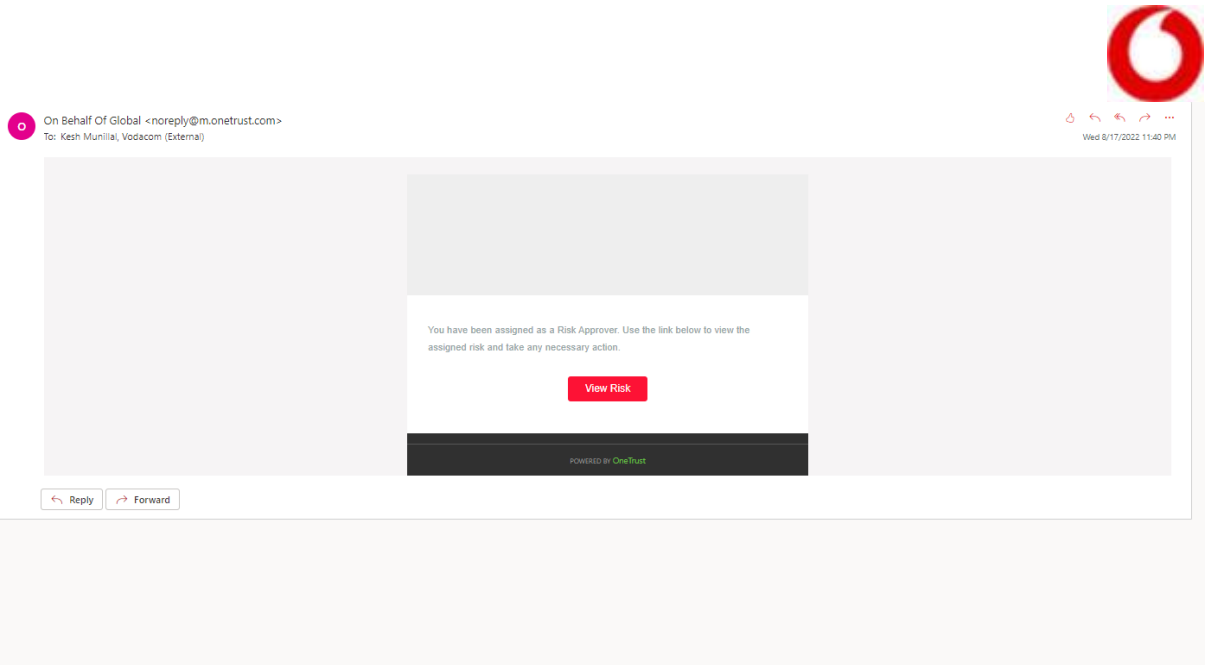


Figure 123

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

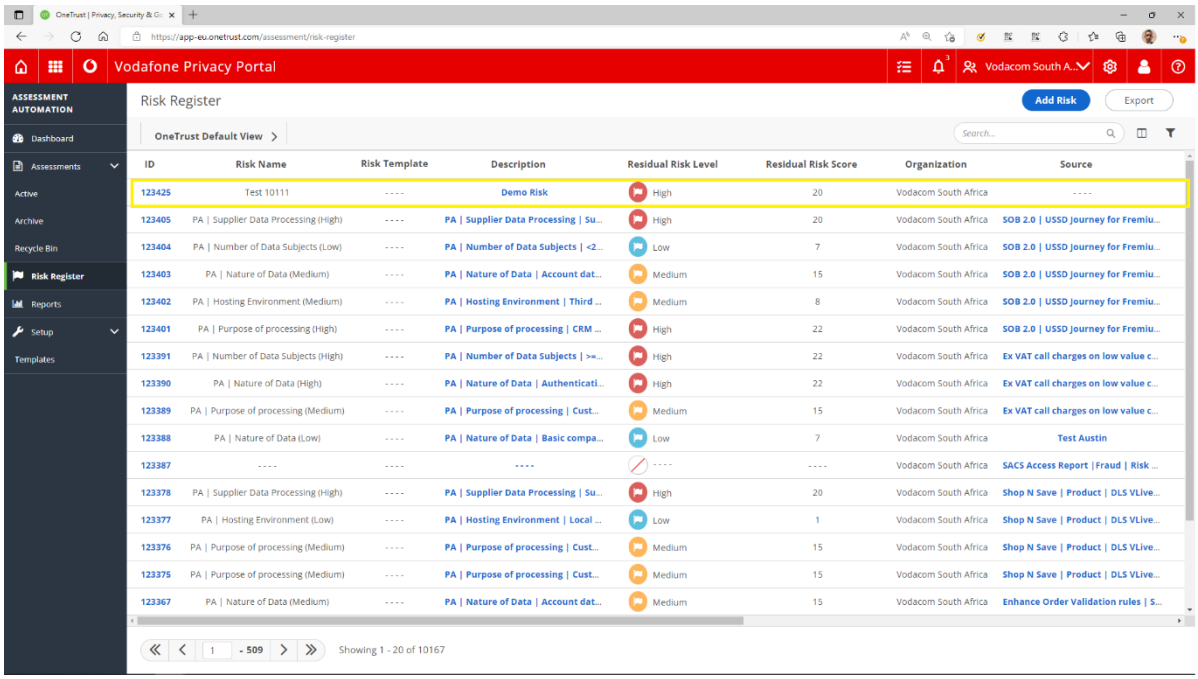


Figure 124

The Risk is displayed

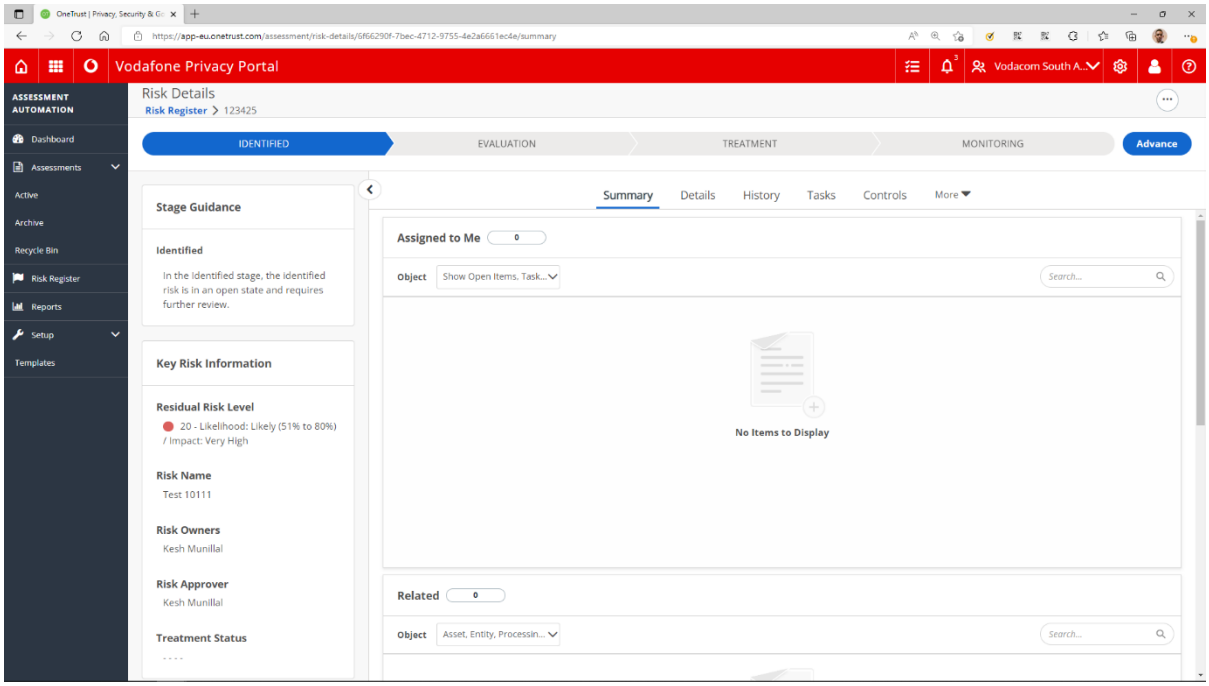


Figure 125

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

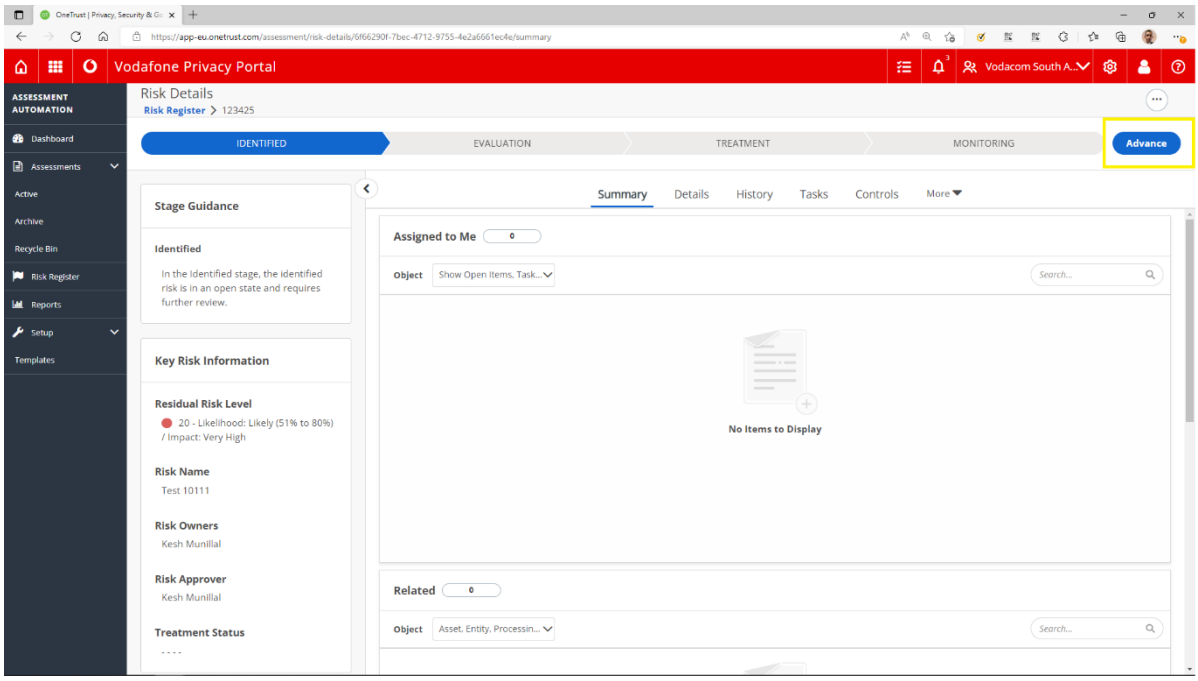


Figure 126

The Risk will be moved along to ‘Evaluate’

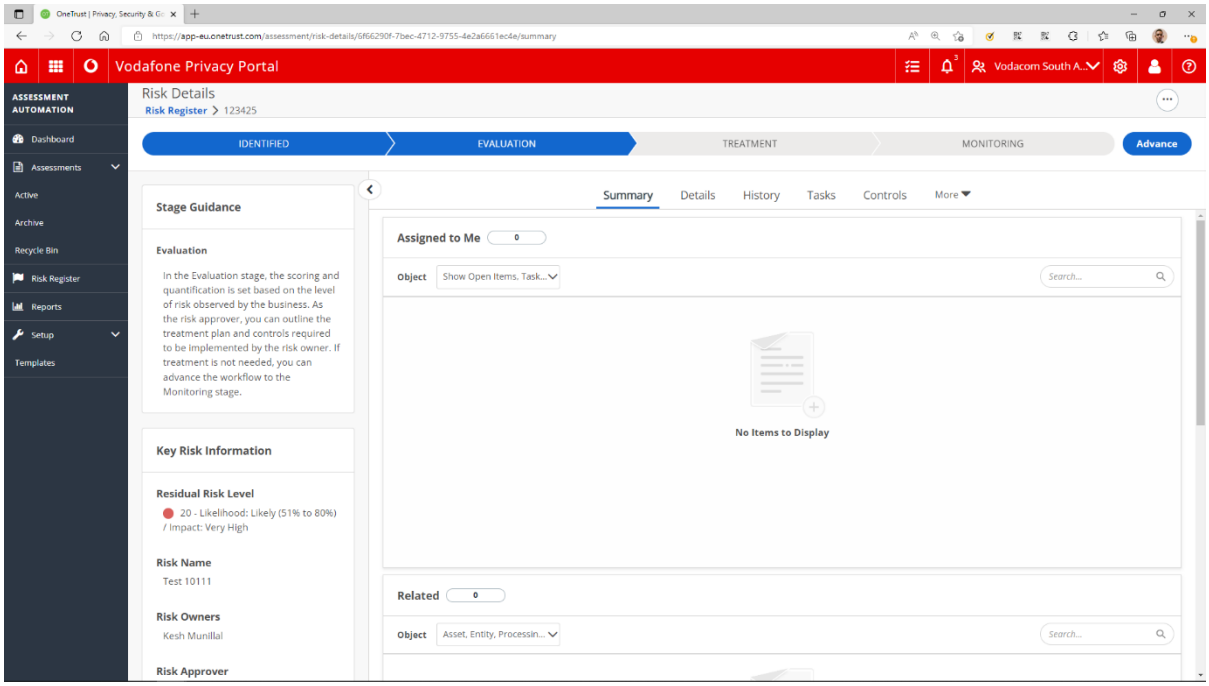


Figure 127

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

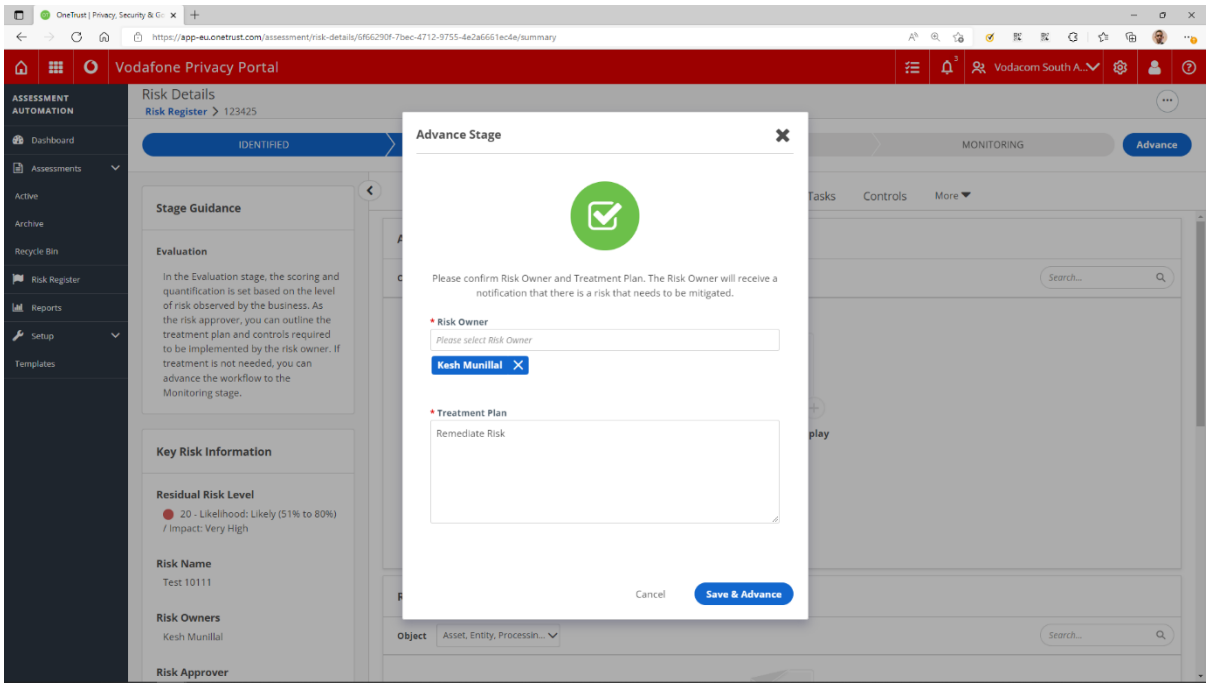


Figure 128

The CSO will be prompted to save the Risk and advance

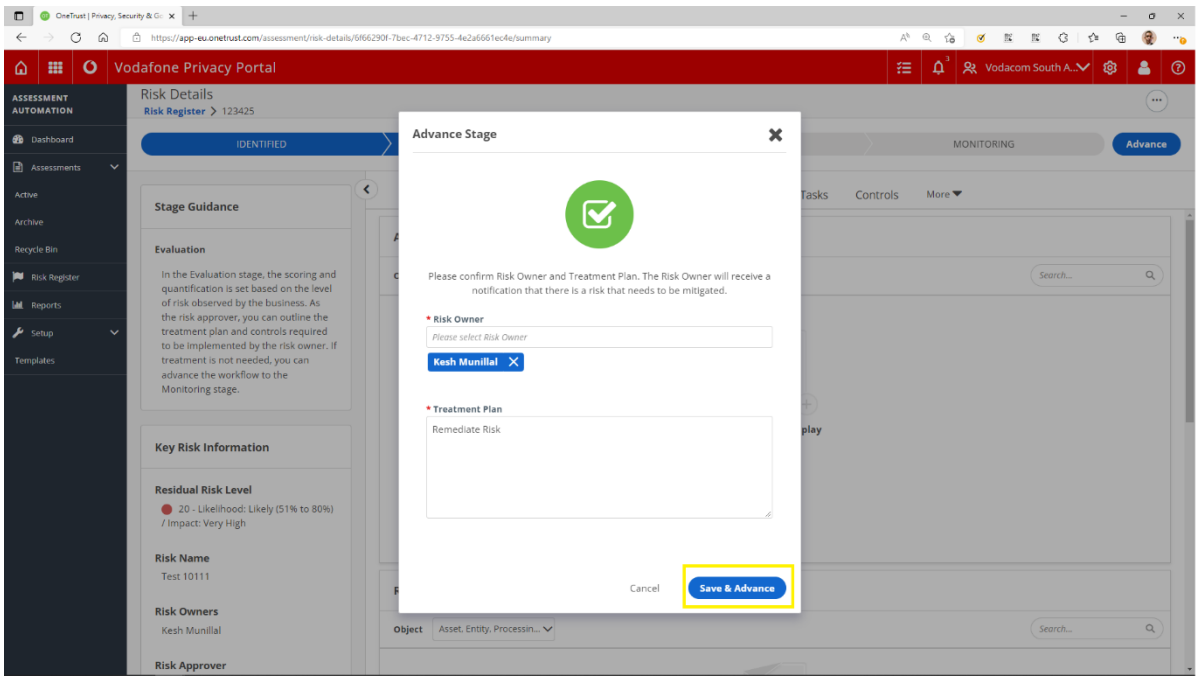


Figure 129

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

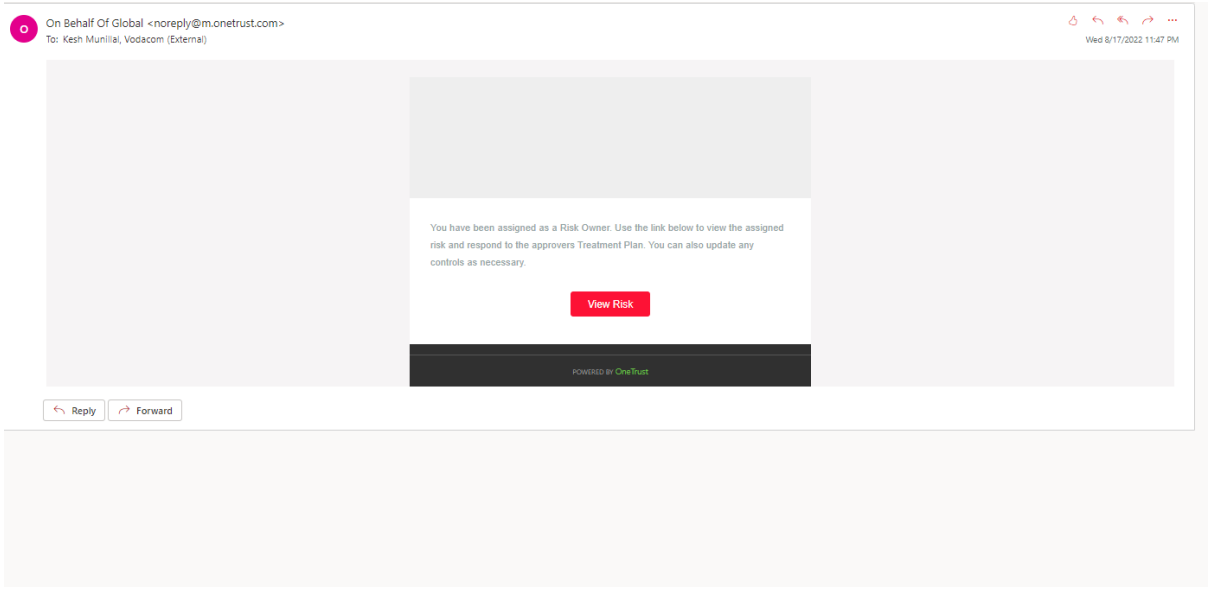


Figure 130

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

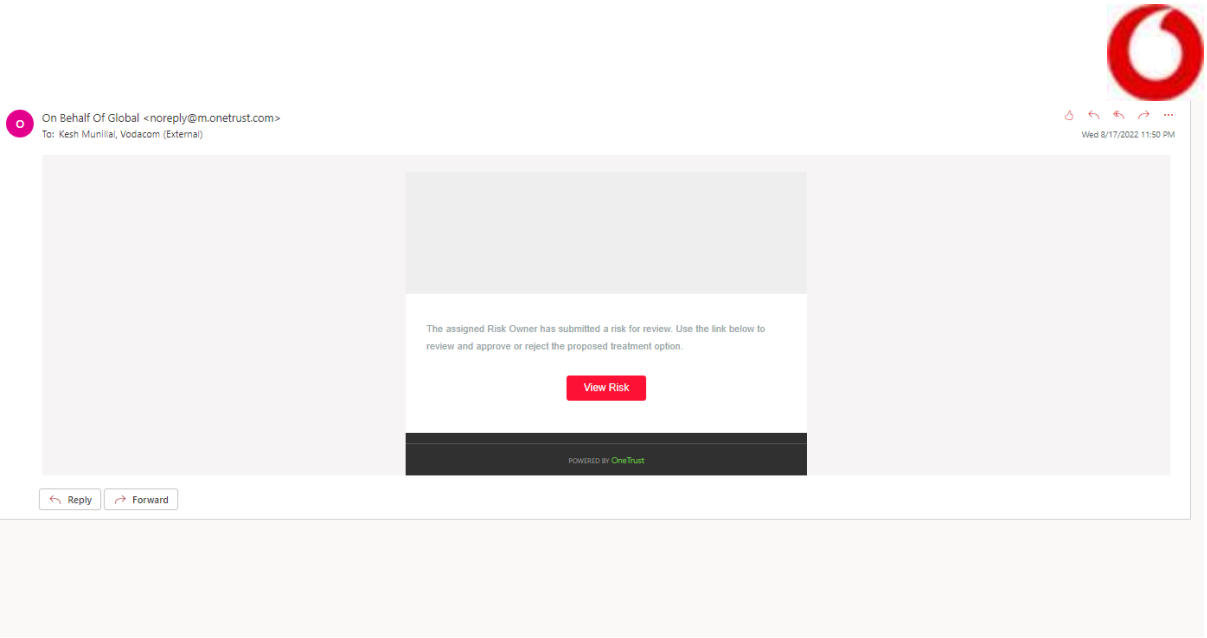


Figure 131

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

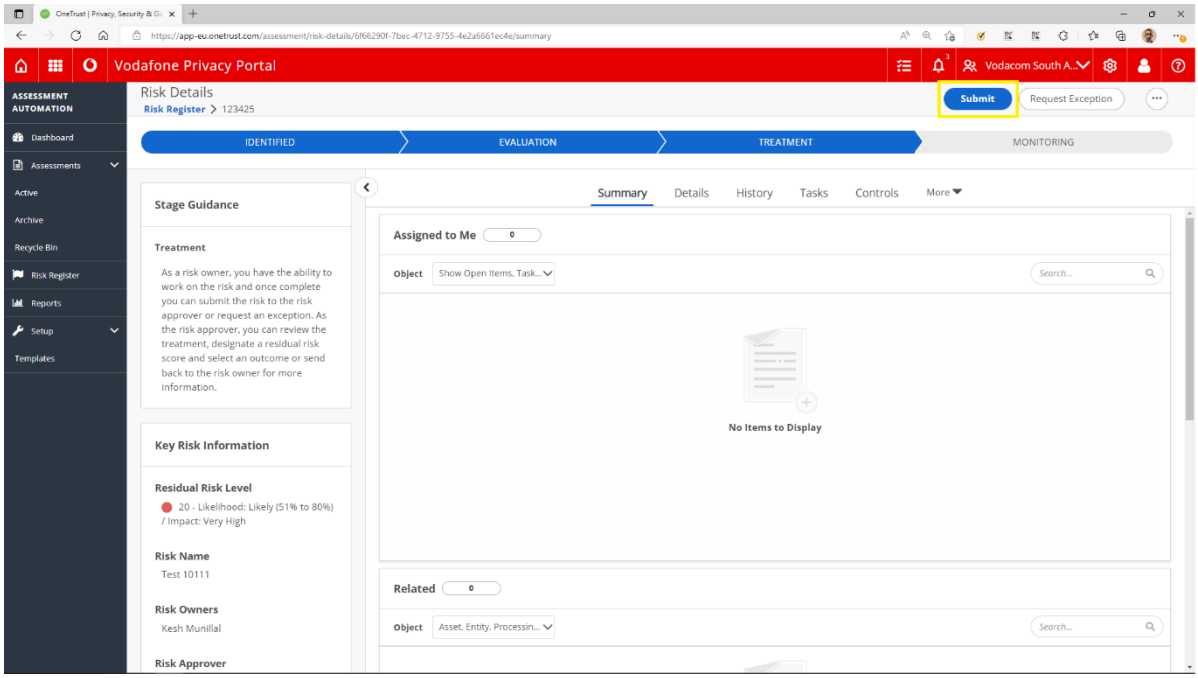


Figure 132

The ‘Submit Treatment Plan’ box will be displayed

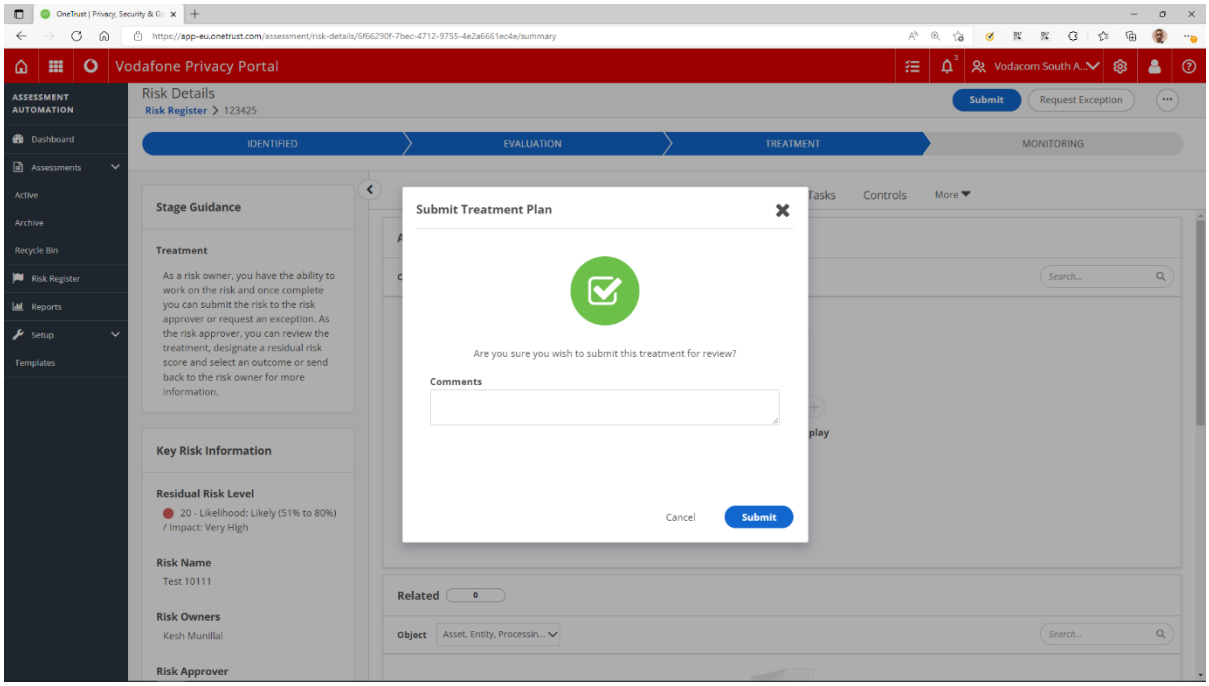


Figure 133

Select the blue ‘Submit’ button

The CSO then may Approve the Treatment Plan

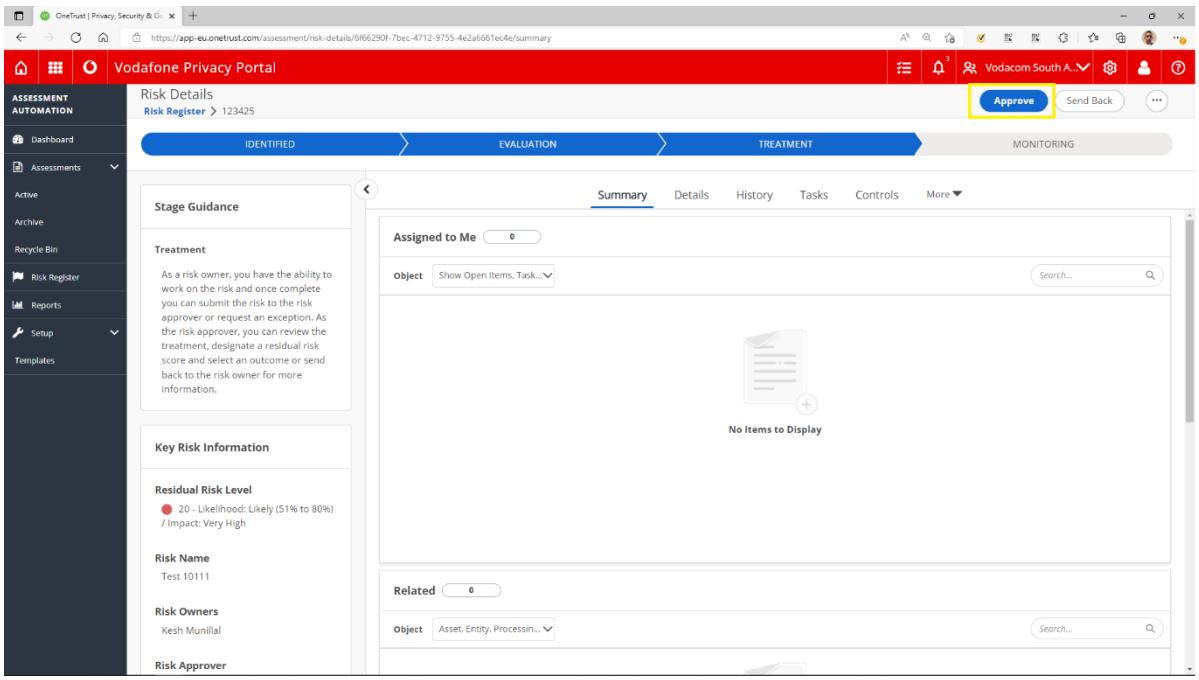


Figure 134

The CSO captures the required information and selects the blue ‘Confirm’ button

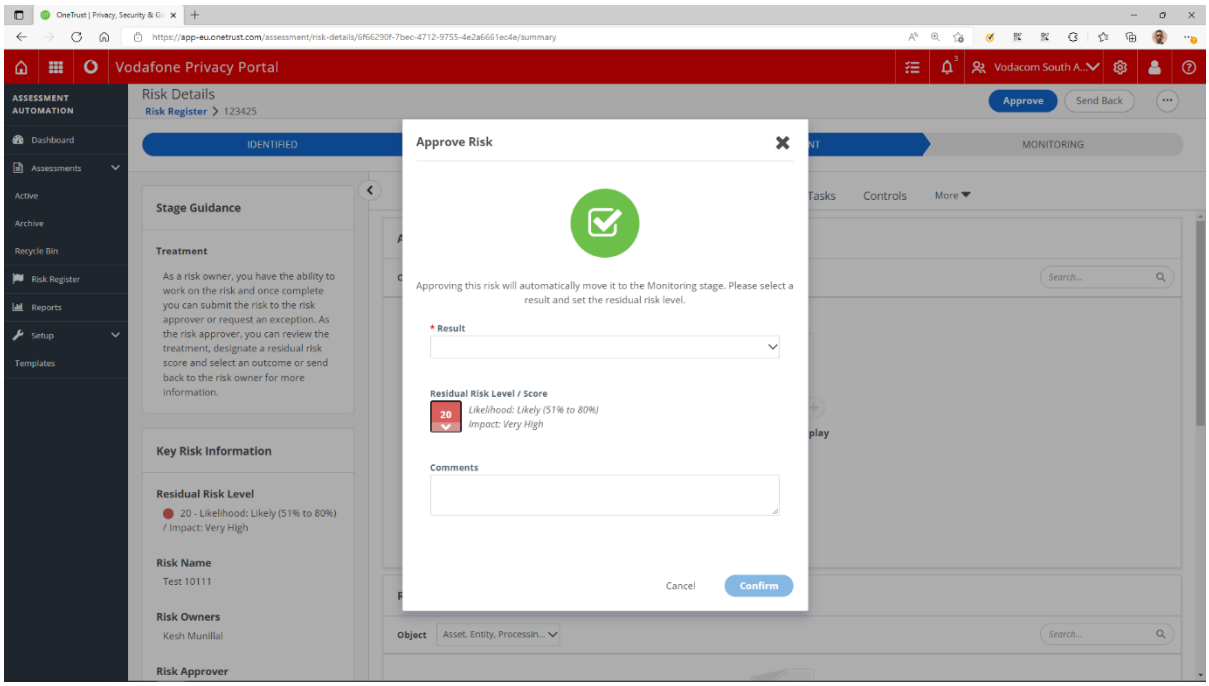


Figure 135

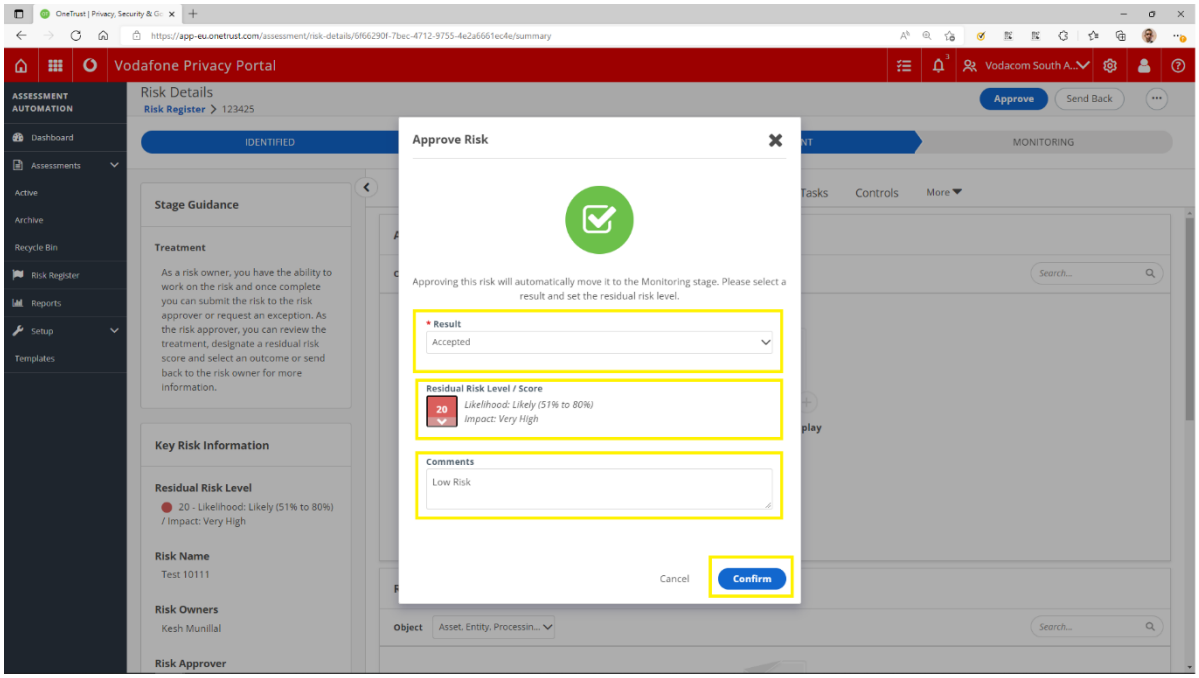


Figure 136

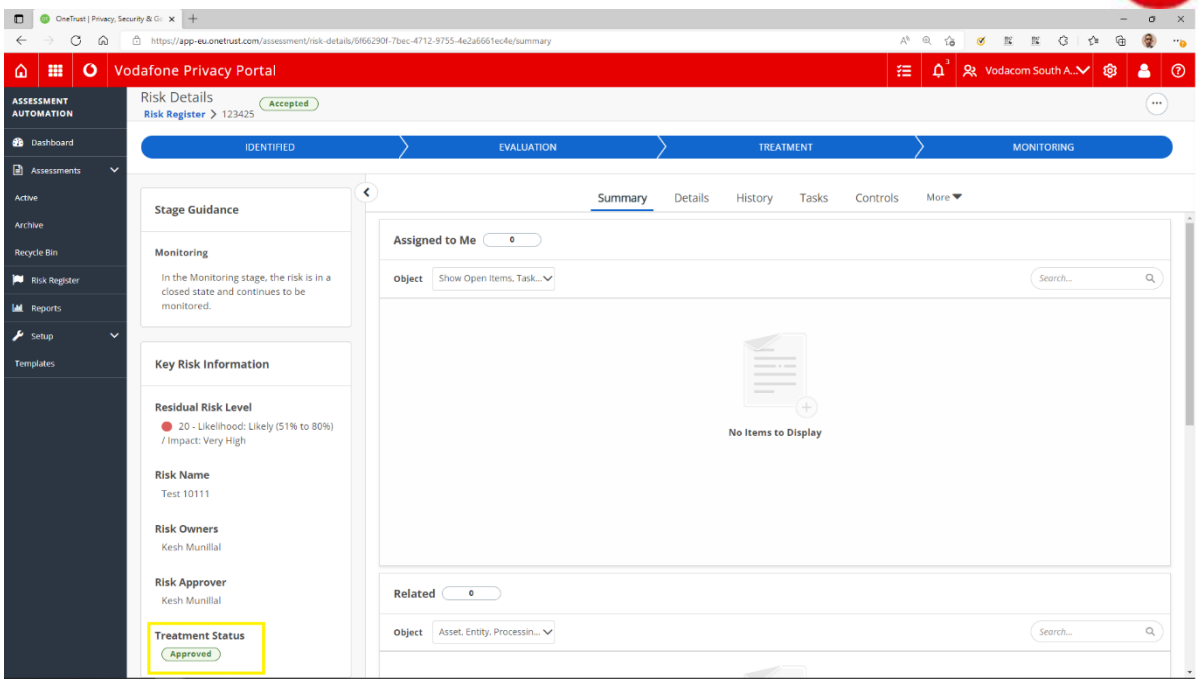


Figure 137

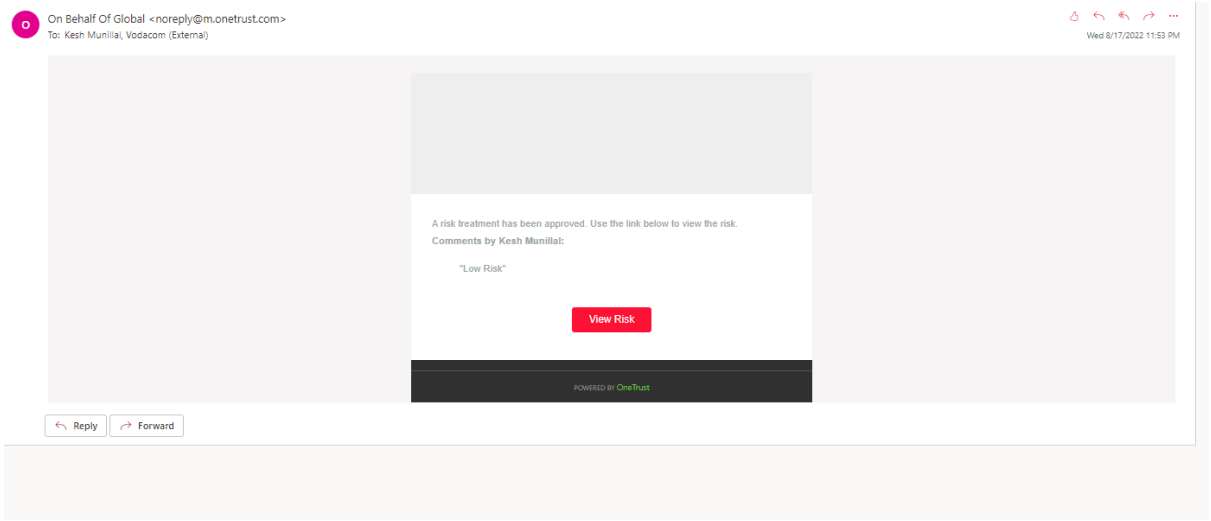


Figure 138

6.1 Risk Register

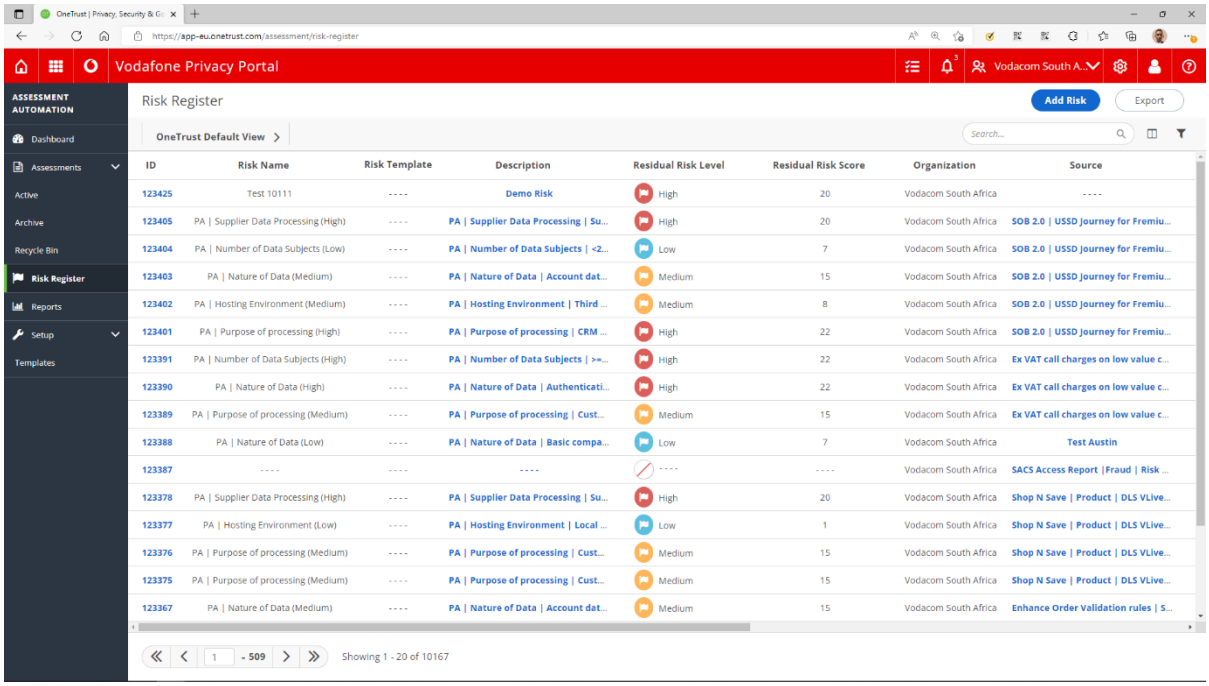


Figure 139

7. Decommissioning

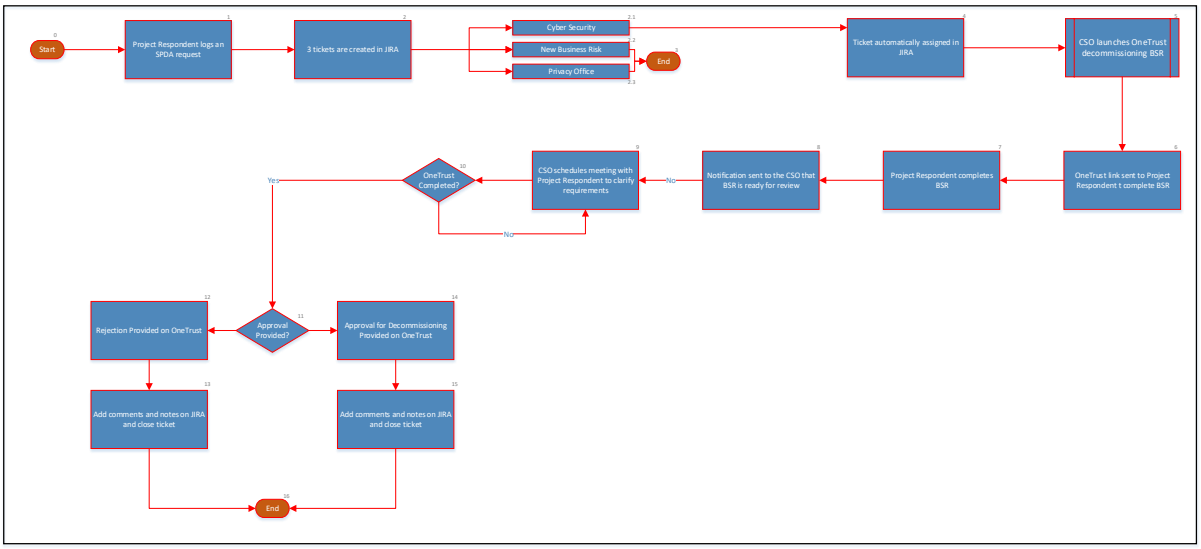


Figure 140

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 competing 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

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.


Decomissioning process.vsdx

Decomissioning process.pdf

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

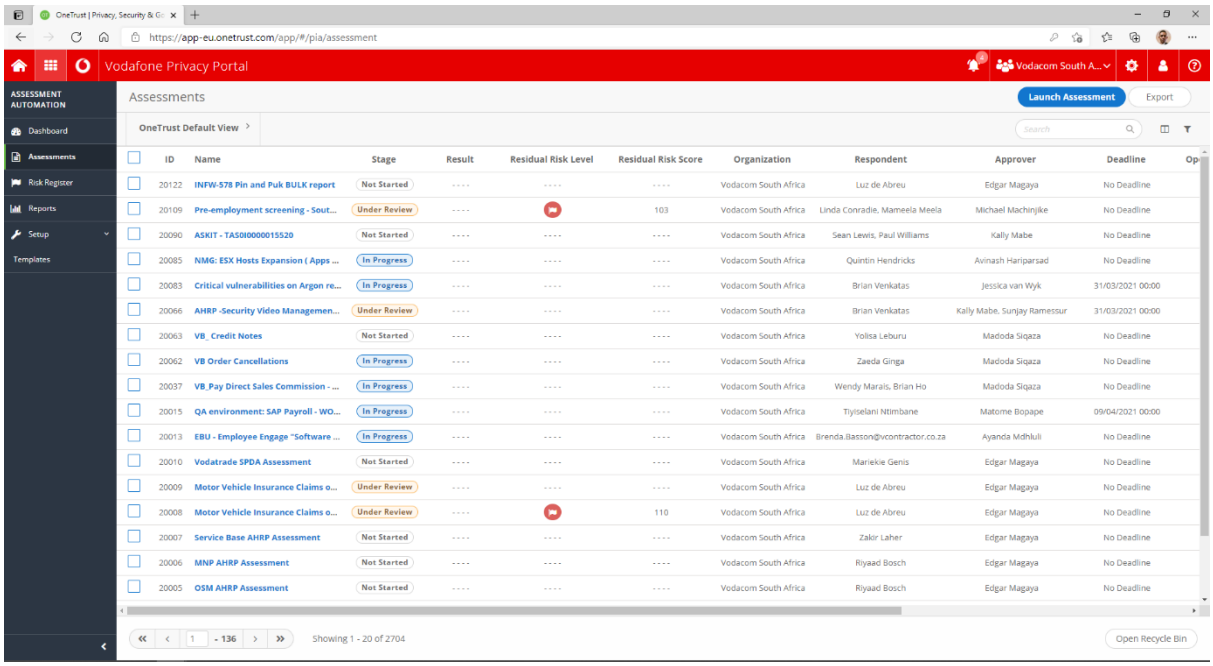


Figure 141

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

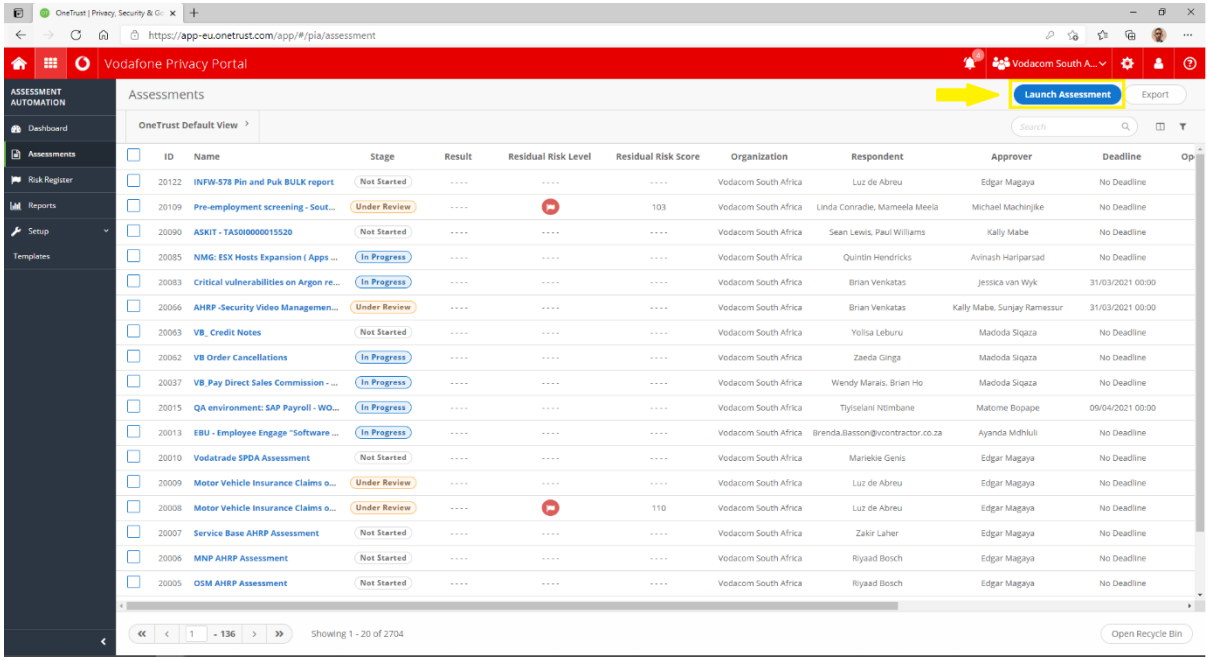


Figure 142

The 'VSA Technology Security Decommissioning assessment' is selected

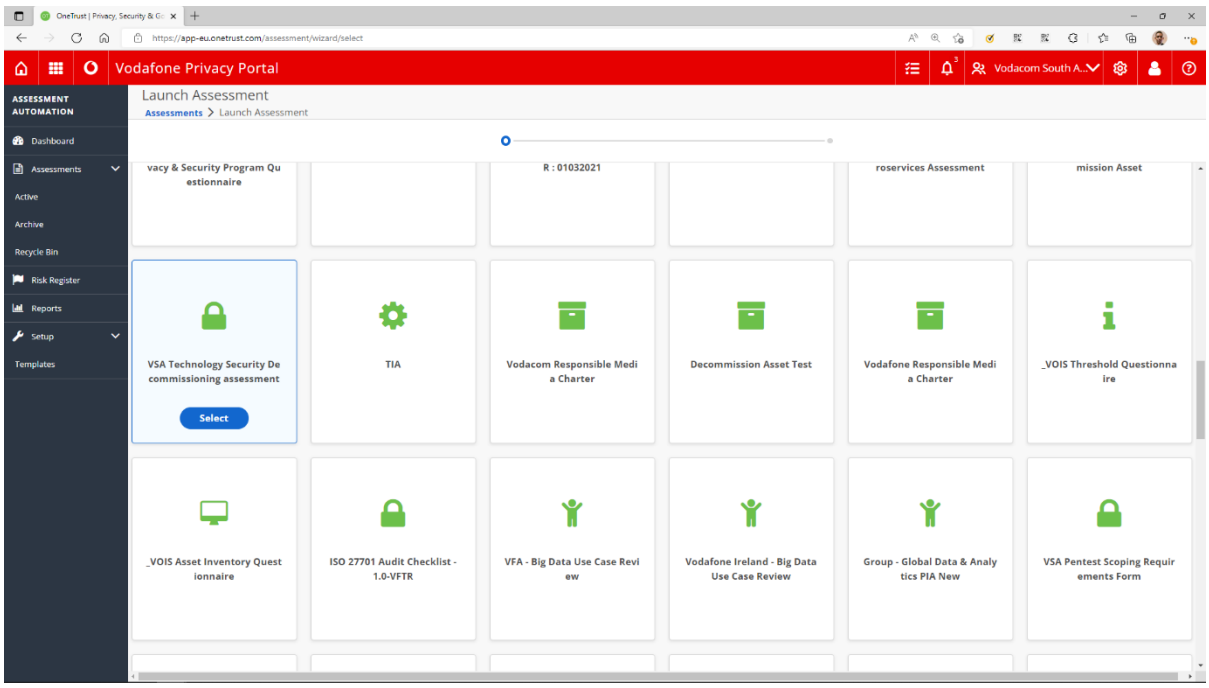


Figure 143

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.

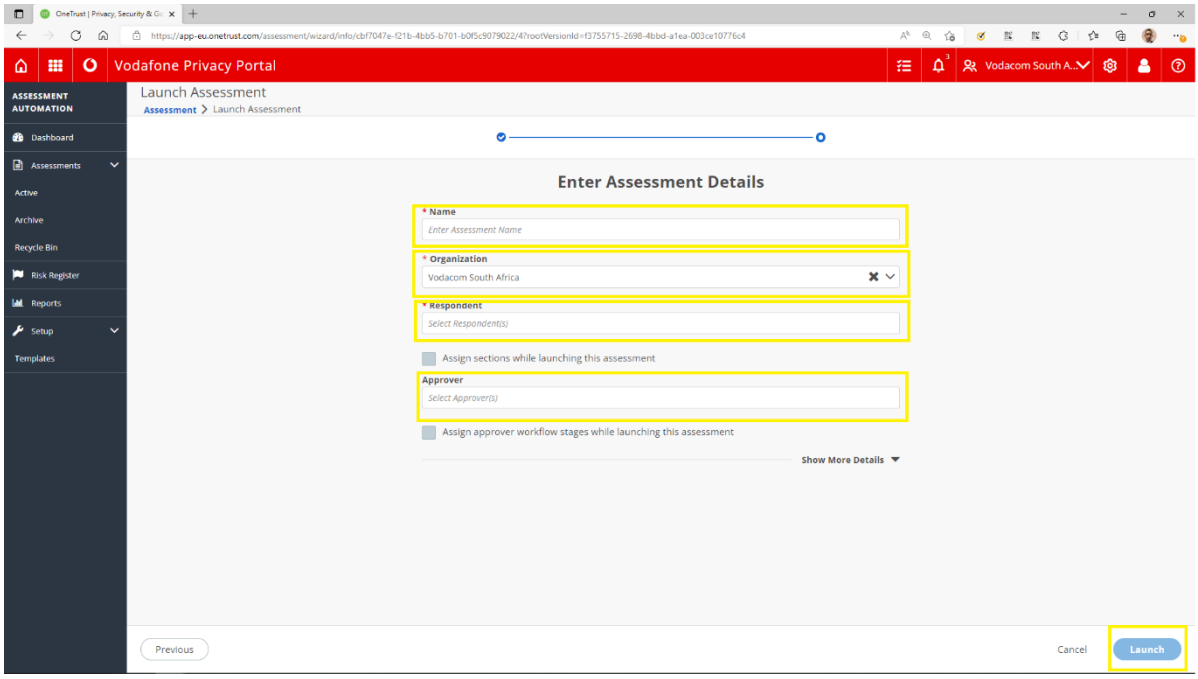


Figure 144

9. OneTrust: Cyber Security Assessment - Decommissioning

9.1 Select Stakeholder and Project Info

Questions 1.1 to 1.5

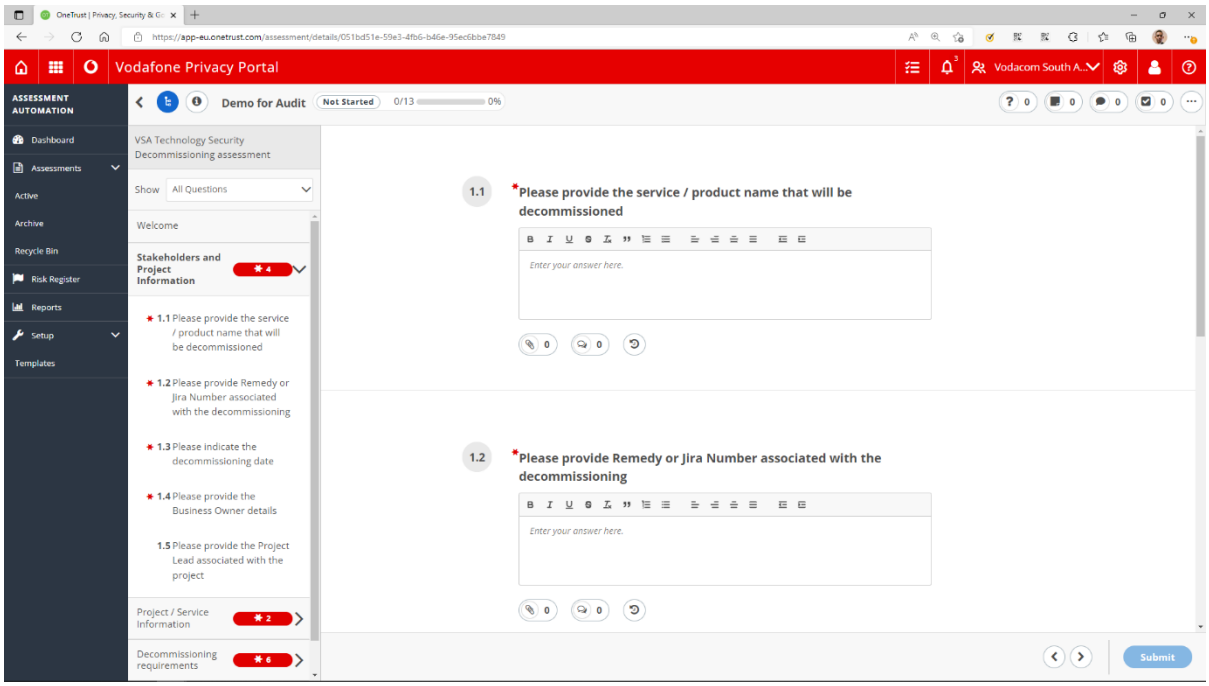


Figure 145

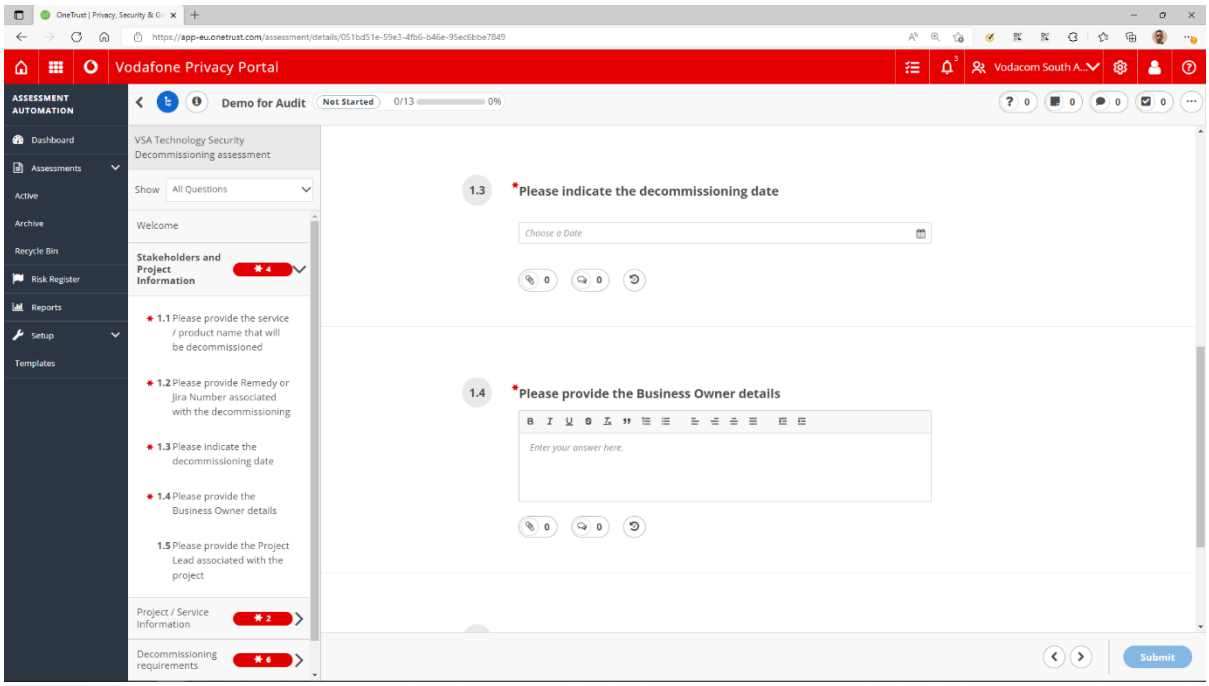


Figure 146

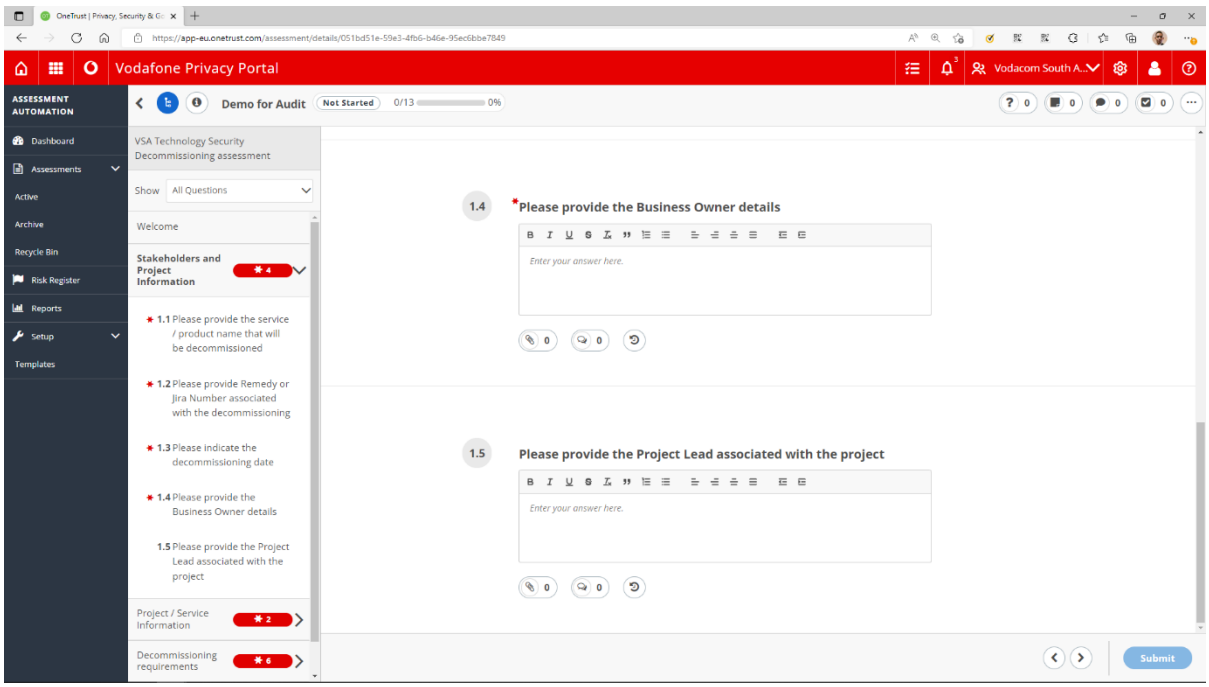


Figure 147

9.2 Project /Service Information

Questions 2.1 to 2.2

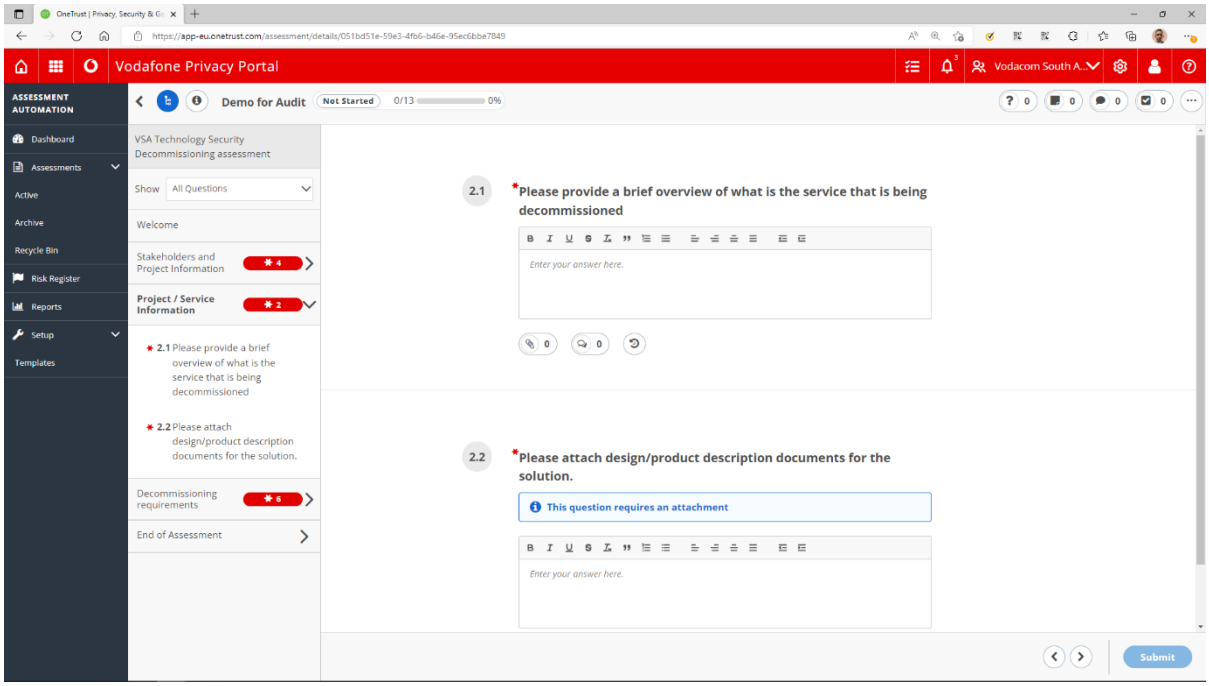


Figure 148

9.3 Decommissioning Requirements

Questions 3.1 to 3.6

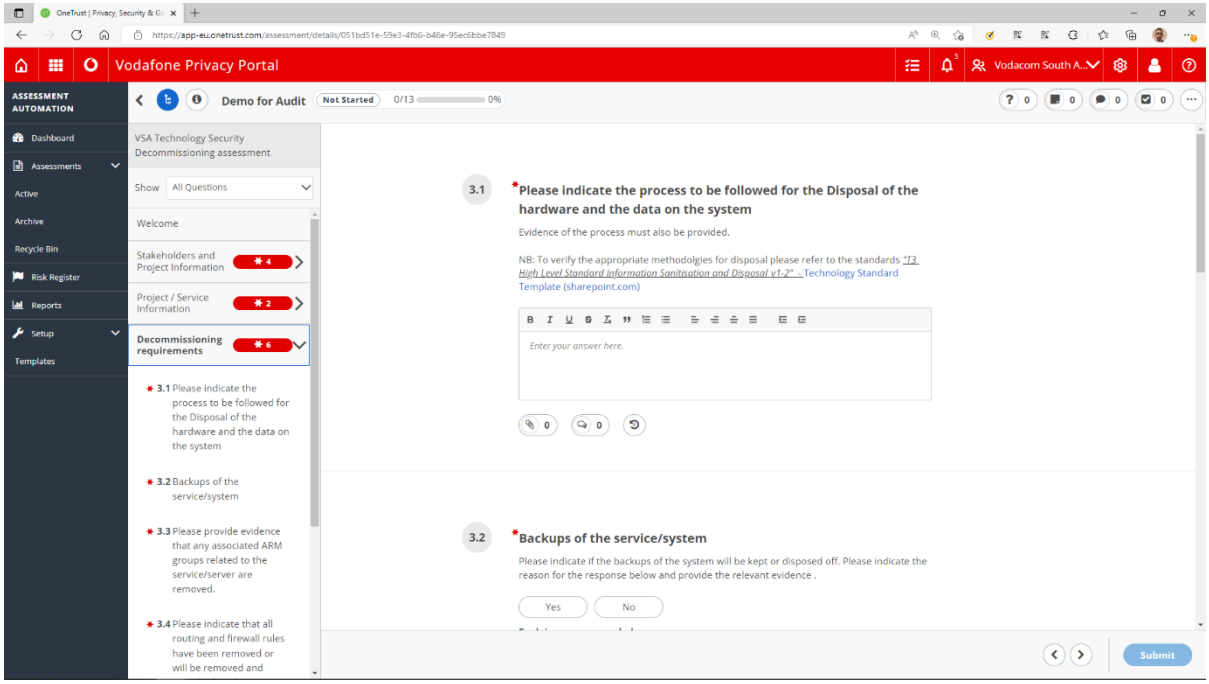


Figure 149

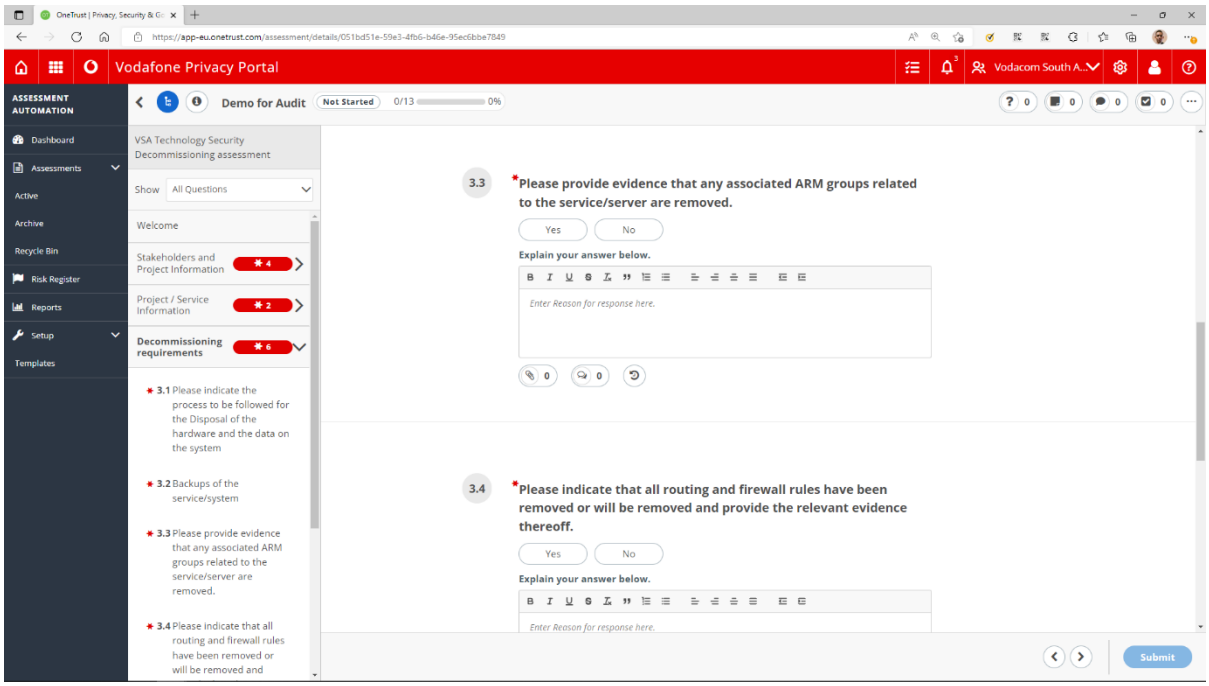


Figure 150

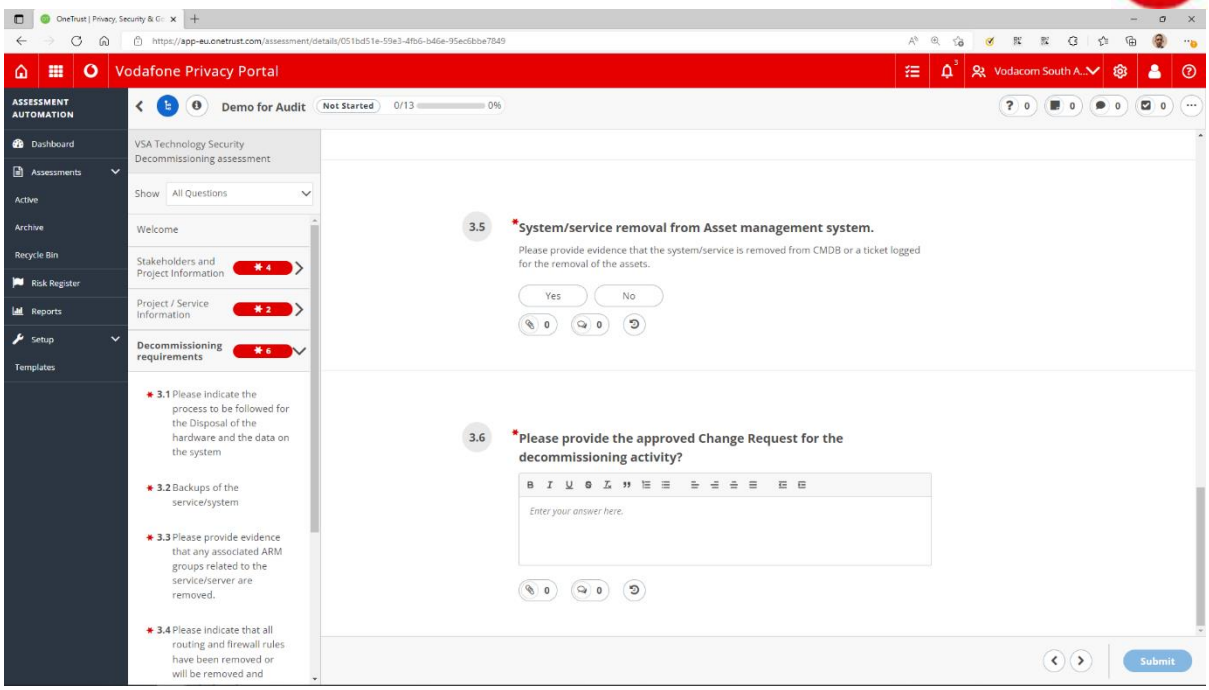


Figure 151

9.4 End of Assessment

Question 4.1

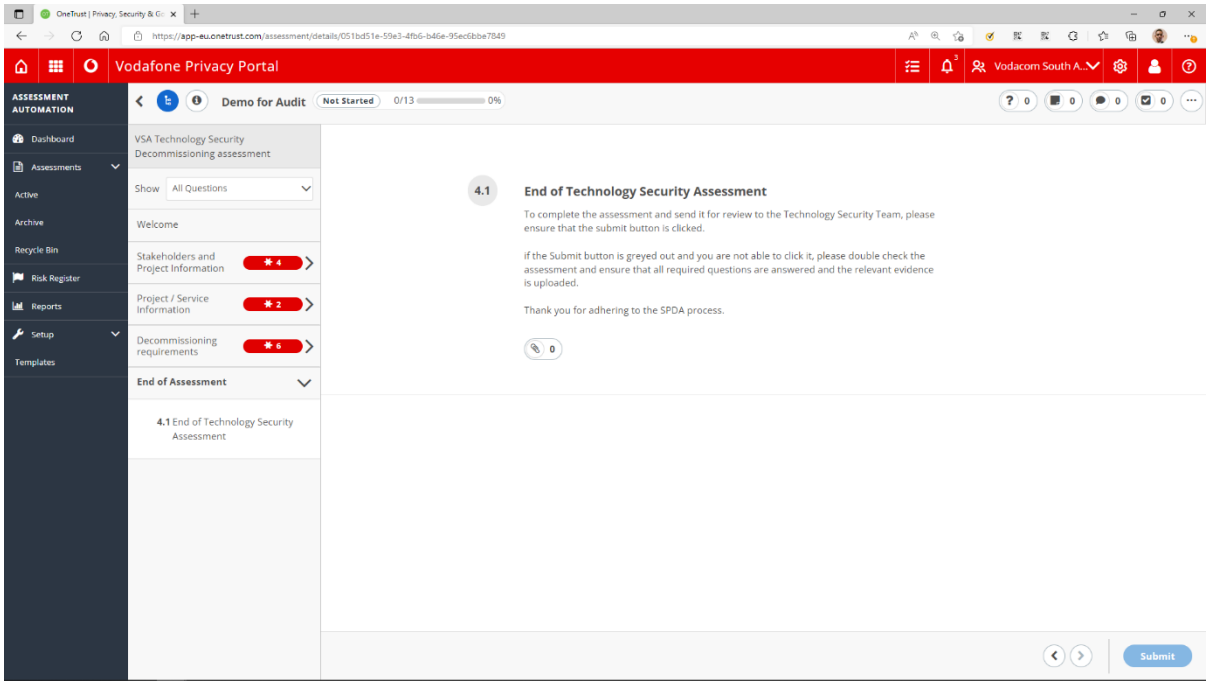


Figure 152

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 3rd 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
		PI\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
			Environment specific CSB assessment required.
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

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: T**he process of strategically prioritizing corrective efforts so that security risks are addressed

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.

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