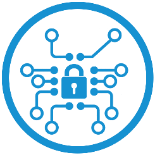
T1

2021

Cyber Security Capability and Maturity Consultancy Services Project

 Functional Specification

ASD ESSENTIAL EIGHT CYBER MIGRATION TOOLKIT

ASD ESSENTIAL EIGHT SIT764 CLASS OF T12020

# 1. Contributors

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Contributor | Summary of Contribution |  |
| 28/5/2020 | Philippa Chong | Draft created and submitted for peer review |  |
| 28/08/2020 | Haddie Harland | Revising deliverables and roles |  |
| 07/10/2020 | Haddie Harland | Updated Testing and Documentation links |  |
| 09/10/2020 | Haddie Harland | Provided project process diagram |  |
| 24/01/2021 | Micheal Cumming | Reviewed prior to consolidation |  |
|  |  |  |  |
|  |  |  |  |

Table 1: Contributors

Table of Contents

[1. Contributors 2](#_Toc52975478)

[2. Project overview 5](#_Toc52975479)

[3. Purpose of overarching documentation 5](#_Toc52975480)

[3.1 Questionnaire and mitigation strategy 5](#_Toc52975481)

[3.2 Front-end and back-end documentation 5](#_Toc52975482)

[3.3 Report documentation 5](#_Toc52975483)

[3.4 Security documentation 6](#_Toc52975484)

[4. Scope 6](#_Toc52975485)

[5. Project Deliverables 6](#_Toc52975486)

[5.1 Phase 1 6](#_Toc52975487)

[5.1.1 Build up familiarity with the ASD Essential Eight 6](#_Toc52975488)

[5.1.2 Propose a solution to practically implement the ASD Essential Eight 6](#_Toc52975489)

[5.1.3 Implement the solution in a low-fidelity prototype of one aspect. 6](#_Toc52975490)

[5.1.4 Develop recommendations and a list of requirements for the product based on this prototype 6](#_Toc52975491)

[5.2 Phase 2 7](#_Toc52975492)

[5.2.1 Produce a minimum viable product based on the requirements determined in the previous phase 7](#_Toc52975493)

[5.2.2 Ensure the internal security of our application is representative of industry expectation 7](#_Toc52975494)

[5.2.3 Complete Real-Client testing and prepare a report and presentation on the findings 7](#_Toc52975495)

[5.2.4 Develop the product further to improve upon MVP in alignment with the results found from the real client testing 7](#_Toc52975496)

[6. Acceptance Criteria 7](#_Toc52975497)

[7. Constraints 8](#_Toc52975498)

[8. Assumptions 8](#_Toc52975499)

[9. System Overview 9](#_Toc52975500)

[9.1 Components 9](#_Toc52975501)

[9.1.1 User interface 9](#_Toc52975502)

[9.1.2 Admin Panel 10](#_Toc52975503)

[9.1.3 Mitigation strategy and Questionnaire 10](#_Toc52975504)

[9.1.4 System Architecture 10](#_Toc52975505)

[10. Project Process 10](#_Toc52975506)

[10.1 Process diagram 10](#_Toc52975507)

[11. Roles and responsibilities 10](#_Toc52975508)

[12. Users 11](#_Toc52975509)

[13. Product Verification 11](#_Toc52975510)

[13.1 Functional Testing 11](#_Toc52975511)

[13.2 User Acceptance Testing (UAT) 11](#_Toc52975512)

[13.3 Real Client Testing 11](#_Toc52975513)

[14. System Security and Integrity Controls 11](#_Toc52975514)

[14.1 Overarching Controls 11](#_Toc52975515)

[14.2 Issue Log 11](#_Toc52975516)

[14.3 Bug Tracker 11](#_Toc52975517)

[14.4 Enhancement Requests (users) 11](#_Toc52975518)

[14.5 Product Security 11](#_Toc52975519)

[15. Go Live Checklist 11](#_Toc52975520)

[Appendices 12](#_Toc52975521)

[User Stories 12](#_Toc52975522)

[Story 1 – Consultant 12](#_Toc52975523)

[Story 2 – Deakin consultancy management 12](#_Toc52975524)

[Story 3 – Developer 13](#_Toc52975525)

[Story 4 - Client 13](#_Toc52975526)

# 2. Project overview

The Cyber Security and Maturity Consultancy Service Project (the Project) aims to research, assess and determine the application of the Australian Signals Directorate (ASD) Essential Eight mitigation strategies, in the small to medium business enterprise business environment.

The tool designed and developed by the Project is a web application, which will assess a client’s security risk profile and offers advice on mitigation strategies as outlined in the ASD Essential Eight. This application utilises these ASD mitigation strategies in a practical sense, creating a tailored report to be used by Deakin’s Australian Cyber Protection Centre consultancy division.

# 3. Purpose of overarching documentation

This project utilises agile principles and methodologies, completing work incrementally in sprints or iterations. In accordance with these principles, this overarching documentation is a live document, which is developed alongside the product as a key project deliverable. In accordance with agile principles, it is a basic document that intends to ensure. that important information is collated but not overstated.

This document also collates the other technical documentation created; a summary of the project’s documentation can be seen below in Table 2.

*Table 2 - Documentation*

|  |  |
| --- | --- |
| **Document File Name** | **Purpose** |
| ASDE8 Overarching Document | Top level documentation |
| ASDE8 Requirements Document | Requirements Documentation |
| ASDE8 Essential Eight User Guide | Guide and business logic including questionnaire and mitigation strategy |
| ASDE8 Questionnaire and Mitigation Strategy | Non-technical Product Definition |
| ASDE8 Frontend and Backend | Architectural documentation for the front-end and back-end |
| ASDE8 Admin Portal | Admin Portal Design Document |
| ASDE8 Reporting | Reporting and PDF Specification |
| ASDE8 New Starter Checklist | Checklist for onboarding new starters |
| *ASD Essential Eight Security Requirements* | *TBD* |

## 3.1 Questionnaire and mitigation strategy

The purpose of the Questionnaire and Mitigation Strategy documentation is to provide current and future users of the SecureBiz product with information about the non-technical aspect of the product. This includes the structure, approach, and scope of the questionnaires, use of the Admin Panel, recommended processes for question refinement and system capabilities related to questionnaire.

This document will equip the user with necessary knowledge to make use of the product tool to determine the maturity level of a client, further analyse the client’s security posture beyond maturity and refine the questionnaire to stay flexible and aligned with the current best advice. The document can be found [here](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Questionnaires%20and%20Mitigation%20Strategies/Questionnaire%20and%20Mitigation%20Strategy%20Documentation.docx?d=wcb0f4ba8413643368c652d10214e813f&csf=1&web=1&e=abYB4w).

## 3.2 Front-end and back-end documentation

The front-end and back-end documentation provides a technical user guide to the front and back-end of the product including the database. It allows users to understand how to add, update features and functionality. The documentation also assists in resolving bugs and also includes architecture and flow diagrams. The document can be found [here](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Front-end%20and%20Back-end%20documentation.docx?d=wcac0e05256664770978301c29e839385&csf=1&web=1&e=OxHhhA).

## 3.3 Report documentation

The report documentation contains the technical aspects of the report collation and coding. This report is contained within the front-end and back-end documentation [here](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Front-end%20and%20Back-end%20documentation.docx?d=wcac0e05256664770978301c29e839385&csf=1&web=1&e=OxHhhA).

In addition to this, user references can be found within the Questionnaire and Mitigation Strategy Documentation [here](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Questionnaires%20and%20Mitigation%20Strategies/Questionnaire%20and%20Mitigation%20Strategy%20Documentation.docx?d=wcb0f4ba8413643368c652d10214e813f&csf=1&web=1&e=abYB4w).

## 3.4 Security documentation

The security documentation will be established in order to contain the important security considerations for the project. This project has the capacity to cause significant harm to businesses if their security vulnerabilities are leaked and therefore security an essential consideration to be done before live testing or deployment.

A security review has been undertaken on the product in it’s current state, with intention to be implemented in the T2 2020 trimester. The security review can be found [here](https://teams.microsoft.com/l/file/26F65153-EF63-40BB-BE42-0EC2027F4E22?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FT2%202020%20Files%2FApplication%20Security%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%20Risk%20Assessment%20Report%20.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

# 4. Scope

In scope:

* A minimum viable product web application to help identify a client’s security posture
* Questionnaires for the client to answer based on the ASD Essential Eight Model
* A personalised client report with recommendations for mitigation strategies to improve their security posture

Out of scope:

* Implementing the mitigations for the client
* Auditing the maturity of the business or the answers provided
* Directly assessing the security measures in place by accessing the client's devices, networks or software

# 5. Project Deliverables

## 5.1 Phase 1

### 5.1.1 Build up familiarity with the ASD Essential Eight

This is complete.

### 5.1.2 Propose a solution to practically implement the ASD Essential Eight

This is complete. The proposed solution is a web application, with an embedded questionnaire as described in this document.

### 5.1.3 Implement the solution in a low-fidelity prototype of one aspect.

This is complete. A low-fidelity prototype was created using Excel and Visual Basic. The prototype can be found [here](https://deakin365.sharepoint.com/:x:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/T3%202019%20Files/T3%202019%20Junior%20Squad/Questionnaire%20Calc%20v1.3.xlsm?d=w56f8232fd7fe432c964f1a98197bb5cf&csf=1&web=1&e=vPvgLm), and a document which discusses the outcome of the prototype can be found [here](https://teams.microsoft.com/l/file/4EE22E4E-4932-49CE-A4CB-E5934E0FEB8B?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FT1%202020%20Files%2FJunior%20Team%2FIndividuals%2FHaddie%2FNotes%20from%20review%20of%20Senior%20Prototype.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

### 5.1.4 Develop recommendations and a list of requirements for the product based on this prototype

This is complete.

A minimum viable product of a web application. This will include:

* A series of Base questions (questions derived from the ASD Essential Eight Maturity Model to determine a client’s maturity level)
* A series of Extended questions (broader questions that influence the recommendations report)
* A customised report containing maturity level calculations and recommendations to achieve ASD Essential Eight Maturity Level Three
* An administrative panel/area that allows for changes to the extended questions, calculations, mitigation strategies and outputs (report)

The web application must be usable on a desktop, laptop, tablet and mobile phone.

Appropriate documentation including:

* Documentation for deployment (Front-end and Back-end)
* User guide and maintenance (Questionnaire and Mitigation, and Reports)
* Due diligence (Web-application and database security)

The requirements documentation can be found [here](https://teams.microsoft.com/l/file/A9122BEA-026F-428F-B3AB-A98BB294440A?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FT2%202020%20Files%2FProject%20Management%20and%20Documentation%2FDocumentation%2FRequirements%20Documentation.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

## 5.2 Phase 2

### 5.2.1 Produce a minimum viable product based on the requirements determined in the previous phase

This is complete and has been accepted.

### 5.2.2 Ensure the internal security of our application is representative of industry expectation

This is in progress. A review of the security implication of components has been completed and corrections are pending implementation.

### 5.2.3 Complete Real-Client testing and prepare a report and presentation on the findings

This has been completed for one client – Smart Finance.

### 5.2.4 Develop the product further to improve upon MVP in alignment with the results found from the real client testing

These changes will be completed as part of release MVP+1.

# 6. Acceptance Criteria

* Meets the web content accessibility guidelines (WCAG)
* Client data is appropriately securely stored/handled or deidentified
* The project itself must meet the security standards in line with the ASD Essential Eight
* The questionnaires must be based on the ASD Essential Eight and effectively measure adherence to them
* The coding logic for determining maturity levels must be correct
* The question logic for determining maturity levels must be correct
* Once an assessment has been completed, a customised report containing maturity level calculations and recommendations is created and is accurate
* The user interface must be usable on desktop, laptop, tablet and mobile phone.
* It must be possible to amend the questions, calculations and outputs
* Project must meet any Deakin Cyber Security Capability and Maturity Consultancy Services guidelines (once the consultancy has been created)

# 7. Constraints

This is a university project and therefore is constrained by the amount of time that the students can dedicate to the subject and their other responsibilities. The project is also constrained in that it currently has no budget and therefore is constrained by cost.

# 8. Assumptions

That Deakin will either provide a server or funding for a server to host the web application when it is complete.

# 9. System Overview

A close up of a map

Description generated with very high confidence

Figure 1: Block diagram of the overall project

## 9.1 Components

The web application has a number of components, as can be seen in the Block Diagram (Figure 1) above.

The system determines the maturity level of a client based on their answers to a series of questions. These questions are split into two categories, **Base** questions and **Extended** questions. The Base questions determine the client’s maturity level, giving them a maturity level between zero and three (with zero meaning the client did not meet any maturity criteria and one to three aligning with the ASD Essential Eight).

The extended questions help understand the client further, based on the ASD Essential Eight and other frameworks in order to provide tailored mitigation advice. The technical aspects of this is discussed in the [*Questionnaire and Strategy Documentation*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Questionnaires%20and%20Mitigation%20Strategies/Questionnaire%20and%20Mitigation%20Strategy%20Documentation.docx?d=wcb0f4ba8413643368c652d10214e813f&csf=1&web=1&e=abYB4w)*.*

The general components of the application are noted below however the technical aspects of the front-end and back-end are dealt with in the [*Front-end and Back-end Documentation*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Front-end%20and%20Back-end%20documentation.docx?d=wcac0e05256664770978301c29e839385&csf=1&web=1&e=OxHhhA).

### 9.1.1 User interface

The user interface is accessed through a web browser. It contains the administrative panel, the questionnaires (split into Base and Extended question sets) and a report view.

More details are provided in the [*Front-end and Back-end*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Front-end%20and%20Back-end%20documentation.docx?d=wcac0e05256664770978301c29e839385&csf=1&web=1&e=OxHhhA) *Documentation*.

### 9.1.2 Admin Panel

The Admin Panel allows for the administrator to amend, add and delete questions, business logic, mitigation strategies, recommendations and output. The Admin Panel accessed via the user interface.

More details are provided in both the [*Front-end and Back-*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Front-end%20and%20Back-end%20documentation.docx?d=wcac0e05256664770978301c29e839385&csf=1&web=1&e=OxHhhA)*end Documentation* and the[*Questionnaire and Strategy*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Questionnaires%20and%20Mitigation%20Strategies/Questionnaire%20and%20Mitigation%20Strategy%20Documentation.docx?d=wcb0f4ba8413643368c652d10214e813f&csf=1&web=1&e=abYB4w) *Documentation.*

### 9.1.3 Mitigation strategy and Questionnaire

The mitigation strategy recommendations and questionnaires are stored in the database. The questions can be amended via Admin Panel (noted above). The questionnaire is filled out by the consultant using the client’s information via the user interface. The maturity level calculator collates the responses from the questionnaire to determine the maturity level reached. This subsequently produces a set of tailored recommendations for effective implementation of the mitigation strategies.

More details are provided in the [*Questionnaire and Strategy*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Questionnaires%20and%20Mitigation%20Strategies/Questionnaire%20and%20Mitigation%20Strategy%20Documentation.docx?d=wcb0f4ba8413643368c652d10214e813f&csf=1&web=1&e=abYB4w) *Documentation.*

### 9.1.4 System Architecture

The web application is hosted on a server (where is yet to be determined). The website is connected to a MongoDB database, which stores the questions, mitigation strategies, the maturity level/business logic and un-identified client responses.

Further information on the database, the framework, platforms and programming languages and scripts used are discussed in the [*Front-end and Back-*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Front-end%20and%20Back-end%20documentation.docx?d=wcac0e05256664770978301c29e839385&csf=1&web=1&e=OxHhhA)*end Documentation*.

# 10. Project Process

## 10.1 Process diagram

The process diagram explains the navigation flow of how the process is functioning in the back-end and front-end when a particular request is generated by the user.

The project process and the process diagram are given in Figure 2.

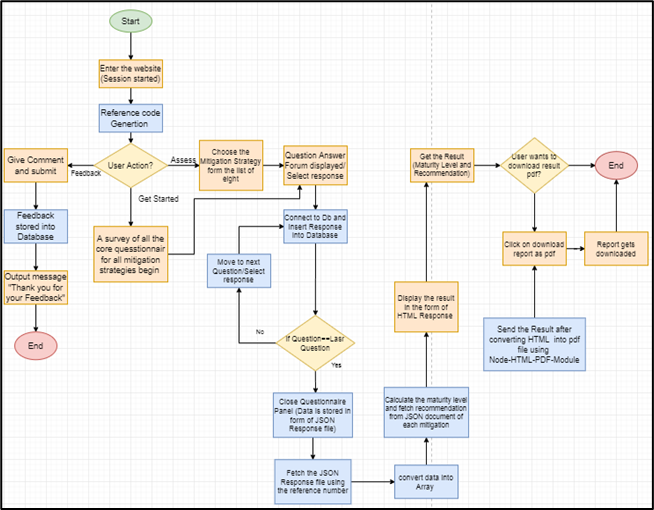


Figure 2: Project process and Process diagram

This diagram is elaborated upon in further detail in the [*Front-end and Back-*](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/Handover%20Artefacts/Front-end%20and%20Back-end%20documentation.docx?d=wcac0e05256664770978301c29e839385&csf=1&web=1&e=OxHhhA)*end Documentation*.

# 11. Roles and responsibilities

As with agile practices each team member is expected and does intermix roles and responsibilities. The roles are described as below:

|  |  |  |
| --- | --- | --- |
| Student |  | Major Contribution |
| Senior Students | | |
|  | Haddie Harland | Management |
|  | Chahat Choudhary | Back-End Build |
|  | Ashley Bawa | Product Design |
|  | Ibrahim Haddad | Application Security |
|  | Kulvinder Kakar | Testing |
|  | Rohan Brahmakshatriya | Front-End Build |
|  | Vanessa Carvalho | Integration |
|  | Vinayaka Karnam | Front-End Build |
| Junior Students | | |
|  | Simon Giang | Back-End Build + Product Design |
|  | Sunny Pannu | Application Security + Testing |
|  | Yemi Babajide | Front-End Build + Management |

# 12. Users

The users of the web application are:

* Deakin’s Cyber Security Consultancy staff
* Small to medium enterprises

The user stories can be found in Appendix 1

# 13. Product Verification

## 13.1 Functional Testing

Functional testing has been undertaken as the project was built to ensure that the deliverables where met. No specific documentation has been created to track this testing.

## 13.2 User Acceptance Testing (UAT)

User acceptance testing was undertaken during Iterations 0, 1, 2 and 3, Trimester 2 of 2020. The results can be seen in the [UAT Documentation](https://teams.microsoft.com/l/file/C9624DDE-D401-4820-9CEC-BAE970096382?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FT2%202020%20Files%2FDeployment%20and%20Testing%2FUAT%20documentation%20for%20Iteration%201%20and%202.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9)*.*

## 13.3 Real Client Testing

Real Client testing was undertaken during Iteration 3, Trimester 2 of 2020. The results can be seen in the [Real Client Test Report – Smart Finance](https://teams.microsoft.com/l/file/00398A17-C554-4DAD-B4E8-AAB043D3D31B?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FT2%202020%20Files%2FDeployment%20and%20Testing%2FReal%20Client%20Testing%20(Smart%20Finance)%2FReal%20Client%20Testing%20report%20-%20Smart%20Finance.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9)*.*

# 14. System Security and Integrity Controls

## 14.1 Overarching Controls

Currently there are no user and security integrity controls except for the ability to revert to an older version of code using GITLab. This item has been backlogged.

## 14.2 Issue Log

Currently there is no issue log, this item has been backlogged.

## 14.3 Bug Tracker

The bug Tracker can be found [here](https://teams.microsoft.com/l/file/280E1E0C-CA11-490C-837D-5229FE5640C6?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=xlsx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FT2%202020%20Files%2FDeployment%20and%20Testing%2FBug%20Tracker.xlsx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

## 14.4 Enhancement Requests (users)

Currently there is no enhancement request ability for users, this item has been backlogged.

## 14.5 Product Security

A security assessment has been completed and can be found [here](https://teams.microsoft.com/l/file/26F65153-EF63-40BB-BE42-0EC2027F4E22?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FT2%202020%20Files%2FApplication%20Security%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%20Risk%20Assessment%20Report%20.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

# 15. Go Live Checklist

Currently there is no go live checklist and the project is not ready to go live. This item has been backlogged.

# Appendices

Appendix 1

## User Stories

### Story 1 – Consultant

Consultants are required to visit client and assess their security maturity level and make recommendations for improvement. The client base is Small to Medium Enterprises (SME) that may not have in-house expertise to understand or implement security measures. Consultants need a tool to undertake security assessments and make recommendations to SME’s.

John is a consultant with Deakin consultancy. John likes order and a having a consistent method of evaluating SME security requirements. As a consultant, John wants to sit to an assessment with clients and provide a security report on the spot.

To do this, John needs to visit a client with an application on Tablet or Laptop and be able to guide the client through a series of questions asked in a simple manner. The question set needs to be specific for each client type and be consistent in the flow of question and response. When the questions are complete, John needs to produce a report that provides the client with their level of security maturity and a list of recommendations to bring the client up to a mature state of maturity.

Specifically, John needs:

* An application suitable for use on laptop or tablet;
* Questions to be specific for the type of client;
* Questions to be framed in non-technical way suitable for SME;
* Questions need to follow a logical flow from one to the next and grouped according to topic;
* Responses to questions to be simple yes/no or score;
* Report to graphically illustrate the maturity level; and
* The report needs to produce a list of recommendations to achieve higher maturity levels;

### Story 2 – Deakin consultancy management

Deakin consultancy require their consultants to undertake security assessments in a consistent manner based on management’s pre-defined criteria. This enables a consistent approach to assessing and making recommendations for Small to Medium Enterprises (SME). The tool needs to be portable and provide Deakin consultancy management with metrics to monitor and assess the usefulness of the tool in the field and to enable further improvement.

Jane is a Deakin Manager from the Deakin consultancy division. Jane likes numbers and is of the view – “you can’t manage what you can’t measure” and “if you can’t measure it, you can’t improve it”. As a manager, Jane wants measurements so that she can know about usage patterns and how to improve the application.

When a consultant uses the application, Jane wants the application to record certain statistics and provide a report to management in a summary fashion. The types of statistics of greatest importance relate to the following, and these must be measured:

* Completion rates for questionnaires;
* Questionnaires / consultant;
* Time it takes to run through a questionnaire;
* Application failure rate; and
* Overall client maturity levels on a per industry basis;

### Story 3 – Developer

Deakin Consultancy have an application for use by their consultants to assess Small to Medium Enterprises (SME) security maturity. The application needs to evolve as both Deakin consultancy and their client needs change over time. To enable continuous support, Deakin Consultancy will need ongoing engagement with Developers to enhance the application. These Developers will likely be varied over time, since the application and requirements will evolve over a long period.

Tim is a developer, enlisted by Deakin Consultancy to provide enhancements to the application. Tim is experienced in application development, particularly anything HTML and understands client/server type applications. Tim knows that since, he has not developed the application from scratch, it is important to understand current state. As a Developer, Tim wants to be able to take an existing application, written by others and implement changes requested by Deakin Consultancy to enhance the product for their consultants and clients.

Based on consultant feedback it has been found that the flow of some questions is not logical and confusing clients doing the questionnaire. Also, there is a need for some additional questions to be added. Tim must now incorporate the ability to add questions to an existing question set and change the workflow of questions as they are being asked. This then needs to be tested on a sample group of clients with the consultant to ensure the changes are acceptable.

Tim needs to understand the application in terms of its front-end and back-end design and implementation. He needs to be able to then understand the requirements from Deakin consultancy and translate these into new features and enhancements in the application. He then needs to implement the changes, then test and validate the new features operate as per Deakin consultancy requirements.

To do this Tim needs:

* A detailed diagram of the structure of the various APIs;
* Well commented source code;
* Working knowledge of HTML, CSS, Bootstrap, JavaScript, NodeJS and MongoDB;
* Working knowledge of tools such as Bitbucket, Visual Studio Code;
* User stories applicable for the new features he will implement; and
* A testing plan with real users;

### Story 4 - Client

Small businesses are often the target of cyber criminals trying to trick businesses into clicking on email links that form part of a broader scam to compromise businesses into making payments to associated trusted entities that turn out to be bogus. Business email compromise and ransomware scams are now commonplace. Businesses are unaware or unsure about how they can detect and manage these types of scams.

Natalie is the office manager for small cleaning company. Of late she has received a number of enquiries from her clients who have been requested to change bank details for payments. Natalie is concerned about the growing threat to the business via scams and is worried about the company’s cyber security preparedness and awareness. As an office manager in charge of finances, Natalie wants to know her company’s security preparedness so that the company can protect itself against potential scams.

Natalie’s business is financially tight, and needs an assessment to understand key actions to take. She’d like a quick, easy questionnaire in simple language with no technical jargon that can enable decisions to be made to protect the business. Natalie has approached Deakin Consultancy to undertake the assessment. Natalie’s key expectations of the assessment are:

* Deal in plain English type questionnaire that speaks to her industry;
* Have someone else ask the questions in a logical manner;
* Have someone guide the assessment process;
* Have the process take under an hour for questions and recommendations;
* Provide a simple report graphically that shows areas of recommendation she can take to her management;
* Provide a list of simplified recommendations, implementable by the business; and
* Provide a benchmark to enable further assessment to be compared.