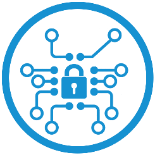


Cyber Security Capability and Maturity Consultancy Services Project

Release Requirements

ASD Essential Eight Cyber Migration Toolkit

ASD Essential Eight SIT782 Class of T22020

2020

# 0. Edits to this document

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Contributor | Summary of Contribution |  |
| 14/09/2020 | Haddie | Original Draft |  |
| 07/10/2020 | Haddie | Implementing Real Client Testing Recommendations |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Figure 0.1: Contributions

Table of Contents

[0. Edits to this document 1](#_Toc52933868)

[1. Introduction 4](#_Toc52933869)

[1.1 Context 4](#_Toc52933870)

[1.2 Releases 4](#_Toc52933871)

[1.2.1 Prototype 4](#_Toc52933872)

[1.2.2 Minimum Viable Product 4](#_Toc52933873)

[1.2.3 Minimum Viable Product Plus One 4](#_Toc52933874)

[1.2.4 Subsequent Releases 4](#_Toc52933875)

[2. Prototype 5](#_Toc52933876)

[2.1 Requirements 5](#_Toc52933877)

[2.1.1 Content 5](#_Toc52933878)

[2.1.2 Infrastructure 5](#_Toc52933879)

[2.2 Product 5](#_Toc52933880)

[2.2.1 Prototype UI 5](#_Toc52933881)

[2.2.1 Questions Back-end 7](#_Toc52933882)

[2.2.1 Report Back-end 7](#_Toc52933883)

[2.2.1 Client Report 7](#_Toc52933884)

[2.3 Review 8](#_Toc52933885)

[3. Minimum Viable Product 9](#_Toc52933886)

[3.1 Requirements 9](#_Toc52933887)

[3.1.1 Content 9](#_Toc52933888)

[3.1.2 Infrastructure 9](#_Toc52933889)

[3.1.3 Documentation 9](#_Toc52933890)

[3.2 Product 10](#_Toc52933891)

[3.3 Review 10](#_Toc52933892)

[3.3.1 UAT 10](#_Toc52933893)

[3.3.2 Real Client testing 10](#_Toc52933894)

[4. Minimum Viable Product Plus One 13](#_Toc52933895)

[4.1 Requirements 13](#_Toc52933896)

[5.1.1 Content 13](#_Toc52933897)

[5.1.2 Infrastructure 13](#_Toc52933898)

[5.1.3 Documentation 13](#_Toc52933899)

[4.2 Product 13](#_Toc52933900)

[4.3 Review 13](#_Toc52933901)

[5. Subsequent Releases 14](#_Toc52933902)

[5.1 Requirements 14](#_Toc52933903)

[5.1.1 Content 14](#_Toc52933904)

[5.1.2 Infrastructure 14](#_Toc52933905)

[5.1.3 Documentation 14](#_Toc52933906)

[6. Works Cited 16](#_Toc52933907)

[7. Appendices 17](#_Toc52933908)

[7.1 Essential Eight Explained 17](#_Toc52933909)

[7.2 Essential Eight Maturity Model 17](#_Toc52933910)

[7.3 Tribe Product Proposal 17](#_Toc52933911)

# Introduction

## Context

This document tracks the project definition and requirements throughout each of its phases, and progressively defines the goals and requirements of subsequent phases. The development of the product has been organised into releases, which are working packages of software that are then assessed to inform the ongoing requirements of the project and define future releases.

## Releases

### 1.2.1 Prototype

The SecureBiz Prototype, Questionnaire Calc V1.3 (QC), was initiated and completed in T3 2019. This release represents the proof of concept for the questionnaire, with a focus on the Restrict Admin Privileges mitigation strategy. Subsequent releases do not reuse any of this code, however the questionnaire was retained and refined for inclusion in the later product.

### 1.2.2 Minimum Viable Product

The SecureBiz minimum viable product, MVP, was initiated in T3 2019 and completed in T2 2020. This release encapsulates the minimum functionality in the intended product format, that is required to represent the product concept. This release covers, at minimum, the breadth of requirements defined by the Prototype review.

### 1.2.3 Minimum Viable Product Plus One

The SecureBiz first revision upon the minimum viable product, release MVP+1, was initiated in T2 2020 and is not yet complete. This release builds on the minimum functionality to address noted gaps with a focus on the application security.

### 1.2.4 Subsequent Releases

Subsequent releases of the SecureBiz product have not yet been planned, but are to be informed by the outcomes of these previous releases. Some items which have not been scoped for MVP or MVP+1 are discussed in this section.

# Prototype

The SecureBiz Prototype, Questionnaire Calc V1.3 (QC), was initiated and completed in T3 2019. This release represents the proof of concept for the questionnaire, with a focus on the Restrict Admin Privileges mitigation strategies. Subsequent releases do not reuse any of this code, however the questionnaire was retained and refined for inclusion in the later product.

## 2.1 Requirements

### 2.1.1 Content

* A set of questions which succinctly cover the requirements to determine the client’s maturity level for the Restrict Admin Privileges mitigation strategy.
* A broader set of questions which gather greater information about the client’s security posture, related to the Restrict Admin Privileges mitigation strategy.

### 2.1.2 Infrastructure

* A basic user interface with which the client can interact, in order to respond to each of the questions.
* Logic which determines the maturity level of the client based on their responses to questions.
* A reporting interface which supplies the processed responses to the questionnaire.

## 2.2 Product

The Questionnaire Calc Prototype consists of a macro-enabled excel file; with four components, each build using excel and visual basic. Each component is represented by a sheet within the excel document.

### 2.2.1 Prototype UI

The “Prototype” sheet is the functional GUI element of the product, containing the questions and the drop downs for the responses from supplied list. The responses are processed on this page as a 1:1 and supply a warning/suggestion if the response is not desirable, or supplies a tick.

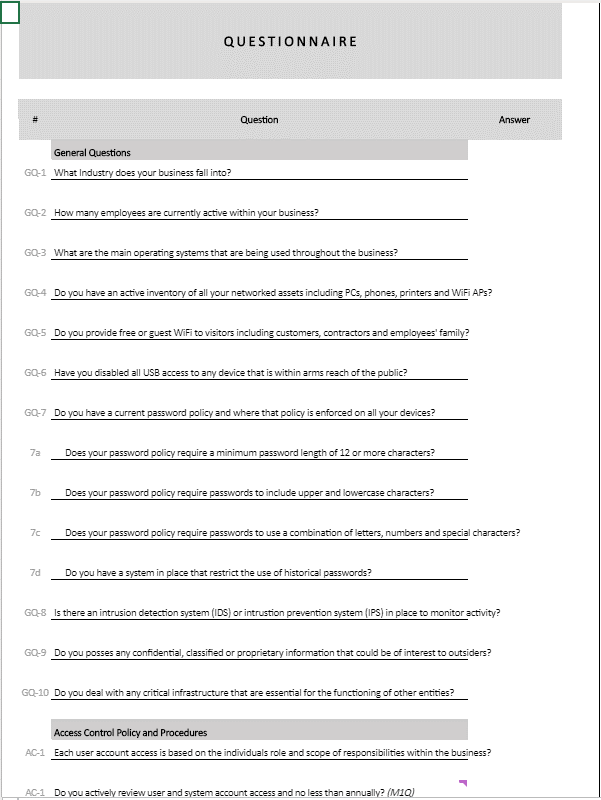


Figure 1: The Prototype Front-end UI, Questionnaire

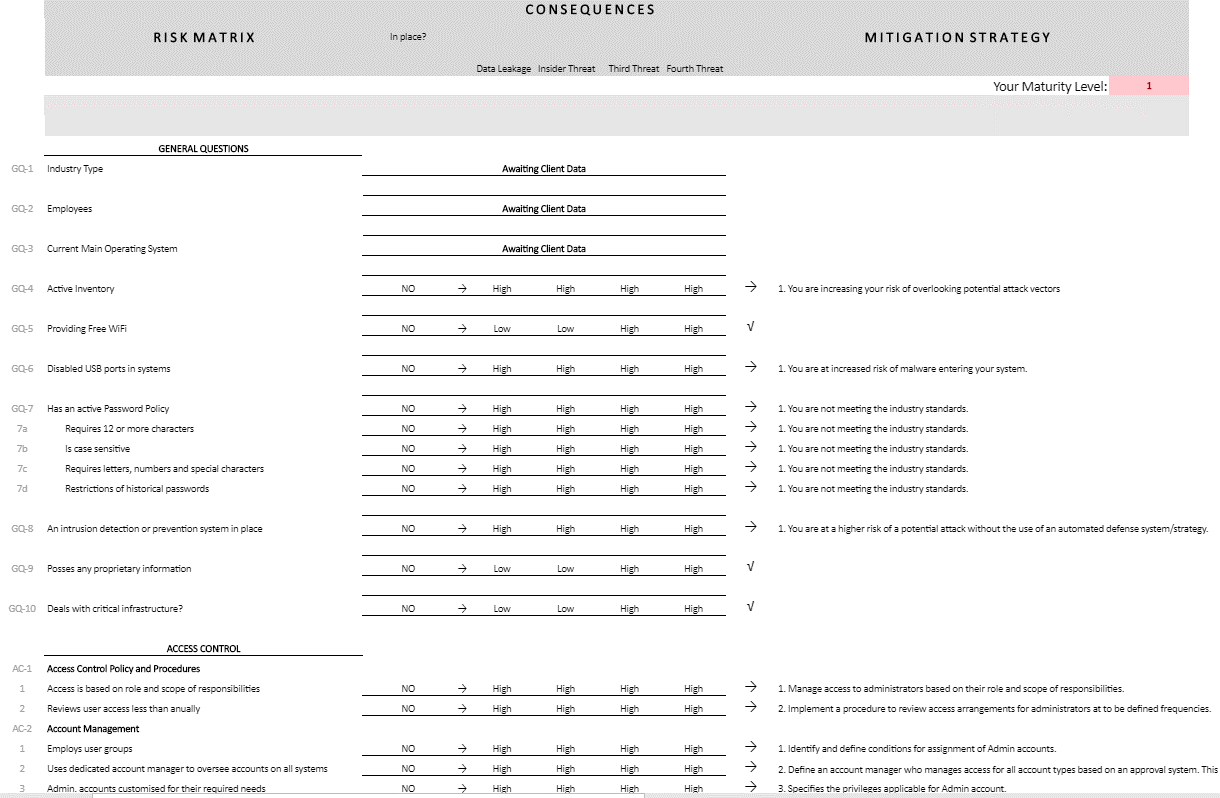


Figure 2: The Prototype Front-end UI, Risks, Consequences and Result

### 2.2.1 Questions Back-end

The “General Question Design” sheet contains the back-end data for the questions, mapping the logic of the results onto the responses provided. Links are an expansion element to redirect clients to existing documentation/tutorials etc for practicing the advice given based on responses for particular questions.

### 2.2.1 Report Back-end

The “Pivot Table Data” sheet Is for the back end of the client report. Most of this is no longer used, the only item specifically in use is for the password item which is displayed as a bar chart.

### 2.2.1 Client Report

The “Client Report” sheet contains the output for the questionnaire, including the resulting maturity level, and simple visuals describing the client’s performance across several specific areas. Most of the client report data is for extension work for client value.

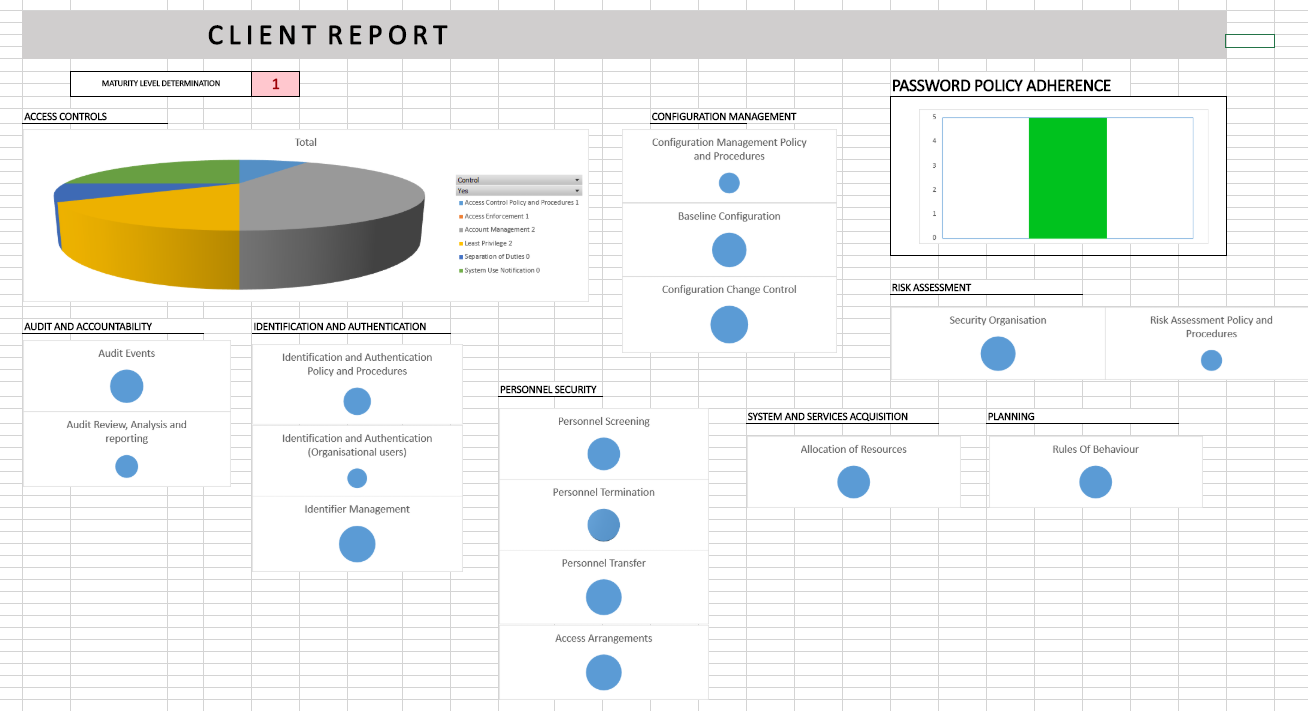


Figure 2: The Prototype Client Report

## 2.3 Review

This prototype has provided a proof of concept for the questionnaire approach. From this, requirements as provided for the subsequent release, MVP, have been produced.

* The product will be web-based using modern website creation techniques.
* The product should provide a succinct analysis of the client’s cyber security posture.
* The product should encapsulate all eight mitigation strategies.
* The product will assess the client based of questionnaire responses and not using any further analysis techniques.
* The product should automatically calculate the maturity level of the client, based on the questionnaire responses provided.
* The product should provide further cyber security advice, based on the questionnaire responses provided.
* The product should be capable of storing client responses.

# Minimum Viable Product

The first release version of the SecureBiz product, MVP, was initiated in T3 2019 and completed in T2 2020. This release encapsulates the minimum functionality in the intended product format, that is required to represent the product concept. This release covers, at minimum, the breadth of requirements defined by the Prototype review.

## 3.1 Requirements

### 3.1.1 Content

* A set of questions which succinctly cover the requirements to determine the client’s maturity level for each of the eight mitigation strategies.
* A broader set of questions which gather greater information about the client’s security posture, related to each of the eight mitigation strategies.
* A set of recommendations for each “incorrect” response to core and extended questions that can be drawn upon to populate the client report.
* Further detail for complex questions, that can be accessed during the questionnaire to provide context and additional information to the user.
* Sufficient question responses that allow for all possible user scenarios, including ‘escape’ responses for non-applicable questions.

### 3.1.2 Infrastructure

* A basic user interface with which the client can interact, in order to respond to each of the questions.
* Logic which determines the maturity level of the client based on their responses to questions.
* A database which stores and retrieves the clients' responses.
* A reporting interface which supplies the processed responses and recommendations based on the product.
* Compatibility with various screen resolutions.
* A "more info" hover node, which provides additional detail to the client to facilitate answering a question.
* The ability to go back and change a question response before the submission of a questionnaire.
* The ability to complete the questionnaire more than once, or to complete a different questionnaire after the conclusion of the first.
* A basic functional UI that is robust against outside-of-clickable-area user iterations

### 3.1.3 Documentation

* A process for tracking changes required for the questions
* A Document which tracks and outlines the questionnaire content and the logic which drives the algorithm
* A Document which provides detail on the technical structures used by the product and the integration between the parts.
* A Document which provides detail on setting up and running the product.
* A document which defines and addresses the security risks associated with all aspects of the product, to protect the user’s data, end-to-end.
* A document that describes the intricacies of the deployment of the product to the cloud.

## 3.2 Product

The product contains 3 components; the Front-end UI, the back-end and the database, represented in various files.

The technical documentation as at the end of Iteration 3 T2 2020, where MVP was complete, can be found [here](https://teams.microsoft.com/_#/school/files/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit?threadId=19%3A1986bd18a5f14a37b6a77545d2b9e0db%40thread.tacv2&ctx=channel&context=Technical%2520Documentation&rootfolder=%252Fsites%252FDeakinCloudVentures-PG%252FShared%2520Documents%252FASD%2520Essential%2520Eight%2520Cyber%2520Mitigation%2520Toolkit%252FT2%25202020%2520Files%252FProject%2520Management%2520and%2520Documentation%252FDocumentation%252FTechnical%2520Documentation).

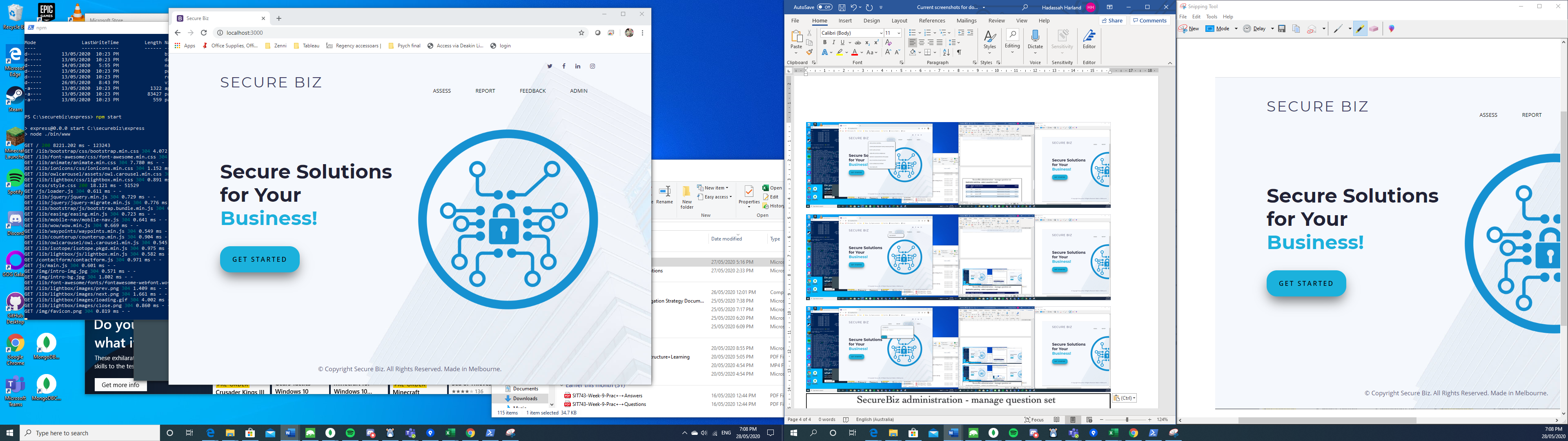


Figure 4: The front-end UI of the SecureBiz product

## 3.3 Review

### 3.3.1 UAT

MVP passed UAT testing in Iteration 3 T2 2020. The report can be found [here](https://teams.microsoft.com/l/file/818C8C76-53BF-4CA0-8553-0983E1A64266?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%2FSecure%20Biz%20UAT%20Sumamry%20report-%20Iteration%203.xlsx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

### 3.3.2 Real Client testing

MVP was put through a round of real client testing with the product Smart Finance. The report can be found here.

The recommendations are as follows:

1. Some concepts covered in questions are unclear – either in context or ambiguity of response. The key objects of the questions should be clearly defined and unambiguous, using simple natural English language.
2. Where natural language is not possible for questions due to the necessity of using a specific term, this term should be clearly defined within the more info hover. Between the question text and more info hover text, there should be no ambiguity in the questions.
3. In some cases a question is not applicable, there should be an option to skip the question or otherwise indicate that it is not applicable. Skipping the question due to being not applicable should then not trigger a “failure” response for the question resulting in the recommendation being appended to the recommendations table.
4. In some cases, a question may be posed as a single question with a single set of responses, but the actual question text contains two questions which need to be considered individually. Questions which contain two elements connected by an “or” or similar language should be evaluated and split if possible, to ensure that every one question has the opportunity for a correctly input response.
5. The question sets are not well-suited to fit a tech start-up company, due to a number of assumptions that are required to make any specific question sets applicable. The most notable example of this is the assumption that the client will be using a self-managed server or workstation when this is not the case for the Smart Finance product nor is it a safe assumption to make about many small tech-startup businesses for which we should be able to apply this product. The assumptions related to each question set and mitigation strategy should be clearly labeled and ideally the questions should be phrased to allow these assumptions to be avoided – ie. The first question asking whether the assumption is satisfied – and then specific advice can be provided to the client based on this response. Ie – if a tech start-up is not using a work-exclusive user profile on their device or a work-exclusive workstation or server, the client should not be asked about the security of this workstation and then given advice on how to improve it, but rather should be provided with lower-level advice that they should be using isolated or exclusive user profiles and workstations to complete this work.
6. If the client completes multiple question sets in the one session – either via assess of via get started, the questions should not be asked again and the response should be retained, for duplicate questions.
7. If the user wished to overwrite question responses, they should then be able to opt to complete the questionnaire again – answering a “Repeat questionnaire and overwrite existing responses?” question to ensure no data is lost without intent.
8. Once the user completes a session, completing a number of different questionnaires, they should be able to extract all the reports from the session into a single HTML/PDF file and choose to send that to themselves rather than needing to stop, save and extract the response feedback each time.
9. In the report, the user is only given the question numbers not the questions themselves, which makes it difficult to go back and reconsider the questions and the responses in context. These questions should be provided on the report.
10. Visual aspects, summaries etc based on the output of the report would be valuable to make the report more accessible and easier to use beyond the heavy amount of text currently used.
11. Explanations of what the maturity levels mean and visuals to help explain this as part of the initial product and additionally as part of the report would be valuable for context for a user that is less familiar with the ASD Essential eight as they otherwise do not necessarily understand what the results they have been provided with mean. For this I would recommend a should explanation of “This means that you have been assessed to be not at all / slightly / mostly/ fully aligned with the advice provided by the ACSC in regards to this mitigation strategy”
12. The mitigation strategies could be grouped by type (preventative, reductive, reparative) with the summaries and visualizations to better leverage the background of the ASD essential eight and provide visual weightings to how important each aspect is. (Some alignment with preventive, reparative and reductive methods is far better than full alignment with only reductive and reparative methods, as the attacks are then not prevented from occurring.)

# Minimum Viable Product Plus One

The SecureBiz first revision upon the minimum viable product, release MVP+1, was initiated in T2 2020 and is not yet complete. This release builds on the minimum functionality to address noted gaps with a focus on the application security.

## 4.1 Requirements

In addition to the requirements of the MVP product, the following requirements are included for the MVP+1 release.

MVP+1 is in development as at the close of T2 2020.

### 5.1.1 Content

* Visualisations and infographic aspects to the client report

### 5.1.2 Infrastructure

* Web deployment of the product

### 5.1.3 Documentation

* Documentation to support the web deployment of the product

## 4.2 Product

The MVP+1 release is still pending.

## 4.3 Review

The MVP+1 release is still pending.

# Subsequent Releases

Subsequent releases of the SecureBiz product have not yet been planned, but are to be informed by the outcomes of these previous releases. Some items which have not been scoped for MVP or MVP+1 are discussed in this section.

## 5.1 Requirements

In addition to the requirements of the MVP product, the following requirements are proposed for future releases.

### 5.1.1 Content

* Review the questions to remove all unnecessary use of jargon or ambiguous terms
* Provide More Info text to all questions that use jargon or ambiguous terms
* Provide ‘Skip Question’ options and reflect this in the report as ‘not applicable’
* Review questions to avoid any assumptions and facilitate skipping of not applicable questions
* Provide the question text to the client as part of the report in addition to the answer and recommendations associated
* Provide a note on completion of the questionnaire to explain what the results printed to screen mean, and that they should look at the report to see recommendations for implementations.
* Provide a note within the report with the final maturity level that briefly explains what it means to have achieved that maturity level and that the user should implement recommendations as according to the report.
* Provide groupings (Preventative, reductive, reparative) to provide context and explanation for the results of each of the eight in the “Get Started” questionnaire results artefacts.

### 5.1.2 Infrastructure

* Support skipping groups of questions that are not applicable based on earlier responses.
* Combine output obtained within a single session into a single compiled and extractable report
* Provide report download with secure options such as encrypted zip files.
* Provide option to overwrite existing responses when answering a questionnaire or question already answered during this session.
* Obscure duplicate questions or provide option to obscure duplicate questions when completing additional questionnaires that contain duplicates, and retrieve the existing response for processing. (Ie. If the user completes Get Started and then completes an assess questionnaire, they should have the option to avoid responding to the base questions again, but the report should still be populated with the noted content.
* Create an ‘about’ page that provides context to what the ASD essential eight are and how the maturity model works
* Save the reports somewhere so they are individually accessible by the client after the client has refreshed the page.

### 5.1.3 Documentation

# Works Cited

Australian Cyber Security Centre, 2020. *Essential Eight Explained.* [Online]   
Available at: cyber.gov.au

Australian Cyber Security Centre, 2020. *Essential Eight Maturity Model.* [Online]   
Available at: cyber.gov.au

Mcmeikan, J., 2019. *ASD Essential Eight Mitigation Maturity Model Toolkit Tribe Product Proposal.* s.l.:Deakin Cloud Ventures.

# Appendices

## Essential Eight Explained

The document can be found locally [here](https://teams.microsoft.com/l/file/7CF71A13-5489-4DDE-88AE-9D16193169B3?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=pdf&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FEssential%20Eight%20Explained%20(April%202019).pdf&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

(Australian Cyber Security Centre, 2020)

## Essential Eight Maturity Model

This document can be found locally [here](https://teams.microsoft.com/l/file/9B60C2B2-1AEB-43CF-B31A-FEBE3D789FE5?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=pdf&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2FASD%20Essential%20Eight%20Maturity%20Model.pdf&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

(Australian Cyber Security Centre, 2020)

## Tribe Product Proposal

This document can be found locally [here](https://teams.microsoft.com/l/file/59A44277-4642-478C-8E5F-7C4A90674192?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%2FSenior%20Team%2FT3%202019%20Files%2FCSRI%20ASD%20Essential%20Eight%20Tribe%20Product%20Proposal%202019%20-%20Working%20document%20260719.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

(Mcmeikan, 2019)