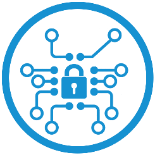


Cyber Security Capability and Maturity Consultancy Services Project

Questionnaire and Mitigation   
Strategy Documentation

ASD Essential Eight Cyber Migration Toolkit

ASD Essential Eight SIT764 Class of T12020

2020

# 0. Edits to this document

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Contributor | Summary of Contribution |  |
| 29/05/2020 | Haddie Harland | Produced initial draft |  |
| 07/10/2020 | Haddie Harland | Added Get Started, Report and Admin panel sections. Removed references to original ‘Report’ button, updated all screenshots. |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Figure 0.1: Contributions

Table of Contents

[0. Edits to this document 1](bookmark://_Toc52933913#_Toc52933913)

[1. Introduction 5](bookmark://_Toc52933914#_Toc52933914)

[1.1 Context 5](bookmark://_Toc52933915#_Toc52933915)

[1.1.1 The Essential Eight 5](bookmark://_Toc52933916#_Toc52933916)

[1.1.2 The Maturity Model 5](bookmark://_Toc52933917#_Toc52933917)

[1.1.3 ASD Essential Eight Mitigation Maturity Model Toolkit Product Tribe 5](bookmark://_Toc52933918#_Toc52933918)

[1.2 Major Purpose of Document 6](bookmark://_Toc52933919#_Toc52933919)

[1.2.1 Management of this document 6](bookmark://_Toc52933920#_Toc52933920)

[2. System Overview 7](bookmark://_Toc52933921#_Toc52933921)

[2.1 The “Get Started” Questionnaire 7](bookmark://_Toc52933922#_Toc52933922)

[2.2 Mitigation Strategy Breakdown and Analysis 7](bookmark://_Toc52933923#_Toc52933923)

[2.3 Feedback form 8](bookmark://_Toc52933924#_Toc52933924)

[2.4 Admin Console 9](bookmark://_Toc52933925#_Toc52933925)

[3. Maturity Assessment 10](bookmark://_Toc52933926#_Toc52933926)

[3.1 Overview 10](bookmark://_Toc52933927#_Toc52933927)

[3.2 The Questionnaire Structure 13](bookmark://_Toc52933928#_Toc52933928)

[3.2.1 Use Cases 13](bookmark://_Toc52933929#_Toc52933929)

[3.2.2 Considerations 14](bookmark://_Toc52933930#_Toc52933930)

[3.3 The Essential Eight 17](bookmark://_Toc52933931#_Toc52933931)

[3.3.1 Application Control 17](bookmark://_Toc52933932#_Toc52933932)

[3.3.2 Patch Applications 18](bookmark://_Toc52933933#_Toc52933933)

[3.3.3 Configure Microsoft Office macro settings 20](bookmark://_Toc52933934#_Toc52933934)

[3.3.4 User Application Hardening 22](bookmark://_Toc52933935#_Toc52933935)

[3.3.5 Restrict Administrative Privileges 24](bookmark://_Toc52933936#_Toc52933936)

[3.3.6 Patch Operating Systems 26](bookmark://_Toc52933937#_Toc52933937)

[3.3.7 Multi-Factor Authentication 28](bookmark://_Toc52933938#_Toc52933938)

[3.3.8 Daily Backups 30](bookmark://_Toc52933939#_Toc52933939)

[3.4 Extension 32](bookmark://_Toc52933940#_Toc52933940)

[4. Making Changes to the Questions 33](bookmark://_Toc52933941#_Toc52933941)

[4.1 Question Change Log 33](bookmark://_Toc52933942#_Toc52933942)

[4.2 Use of Question Change Log 34](bookmark://_Toc52933943#_Toc52933943)

[4.2.1 Adding a Question 34](bookmark://_Toc52933944#_Toc52933944)

[4.2.2 Editing a Question 35](bookmark://_Toc52933945#_Toc52933945)

[4.2.3 Deleting a Question 37](bookmark://_Toc52933946#_Toc52933946)

[5. Reporting 39](bookmark://_Toc52933947#_Toc52933947)

[5.1 Get Started 39](bookmark://_Toc52933948#_Toc52933948)

[5.1.1 PDF Report 39](bookmark://_Toc52933949#_Toc52933949)

[5.1.2 HTML Report 39](bookmark://_Toc52933950#_Toc52933950)

[5.2 Assess 41](bookmark://_Toc52933951#_Toc52933951)

[5.2.1 PDF Report 41](bookmark://_Toc52933952#_Toc52933952)

[5.2.2 HTML Report 42](bookmark://_Toc52933953#_Toc52933953)

[5.3 Providing the results to the client 42](bookmark://_Toc52933954#_Toc52933954)

[6 Admin Portal 43](bookmark://_Toc52933955#_Toc52933955)

[6.1 Manage Mitigation Strategies 43](bookmark://_Toc52933956#_Toc52933956)

[6.2 Statistics 45](bookmark://_Toc52933957#_Toc52933957)

[7 System Capabilities and Constraints 46](bookmark://_Toc52933958#_Toc52933958)

[7.2 Question Duplication 46](bookmark://_Toc52933959#_Toc52933959)

[7.1.1 Summary 46](bookmark://_Toc52933960#_Toc52933960)

[7.1.2 Solution 46](bookmark://_Toc52933961#_Toc52933961)

[7.1.3 Considerations 46](bookmark://_Toc52933962#_Toc52933962)

[7.3 Question Depth 46](bookmark://_Toc52933963#_Toc52933963)

[7.2.1 Summary 46](bookmark://_Toc52933964#_Toc52933964)

[7.2.2 Solution 46](bookmark://_Toc52933965#_Toc52933965)

[7.1.3 Considerations 47](bookmark://_Toc52933966#_Toc52933966)

[7.4 Additional Detail 47](bookmark://_Toc52933967#_Toc52933967)

[7.3.1 Summary 47](bookmark://_Toc52933968#_Toc52933968)

[7.3.2 Solution 47](bookmark://_Toc52933969#_Toc52933969)

[7.1.3 Considerations 47](bookmark://_Toc52933970#_Toc52933970)

[7.5 Response Tracking 47](bookmark://_Toc52933971#_Toc52933971)

[7.4.1 Summary 47](bookmark://_Toc52933972#_Toc52933972)

[7.1.2 Solution 47](bookmark://_Toc52933973#_Toc52933973)

[7.1.3 Considerations 47](bookmark://_Toc52933974#_Toc52933974)

[8 Works Cited 49](bookmark://_Toc52933975#_Toc52933975)

[9 Appendices 51](bookmark://_Toc52933976#_Toc52933976)

[9.2 Essential Eight Explained 51](bookmark://_Toc52933977#_Toc52933977)

[9.3 Essential Eight Maturity Model 51](bookmark://_Toc52933978#_Toc52933978)

[9.4 Tribe Product Proposal 51](bookmark://_Toc52933979#_Toc52933979)

[9.5 Change Management 51](bookmark://_Toc52933980#_Toc52933980)

[9.6 System Capabilities and Constraints solution considerations 52](bookmark://_Toc52933981#_Toc52933981)

[8.5.1 Question Duplication 52](bookmark://_Toc52933982#_Toc52933982)

[8.5.2 Question Depth 53](bookmark://_Toc52933983#_Toc52933983)

[8.5.3 Additional Detail 53](bookmark://_Toc52933984#_Toc52933984)

[8.5.4 Response Tracking 54](bookmark://_Toc52933985#_Toc52933985)

# Introduction

## Context

### 1.1.1 The Essential Eight

The ASD Essential Eight is a list of the eight most valuable strategies to mitigate cyber security incidents, as prioritized by the Australian Cyber Security Centre (ACSC). It consists of eight baseline mitigation strategies which, when implemented, provide a reasonable level of protection against a broad set of cyber security threats. This includes prevention of malware delivery and execution, limiting the extent of incidents when they do occur, and recovering data and system availability after the fact. (Australian Cyber Security Centre, 2020)

The focus points for each of the eight are as below:

* Application Whitelisting
* Patch Applications
* Configure Microsoft Office Macro Settings
* User Application hardening
* Restrict Admin Privileges
* Patch Operating systems
* Multi-factor Authentication
* Daily Backups

### 1.1.2 The Maturity Model

Each of the eight of the Essential Eight list are broken down into a tiered implementation system, which describes how closely an organisation has aligned to the intent of the mitigation strategy. The tiers are given as:

* Maturity Level One: Partly aligned with the intent of the mitigation strategy.
* Maturity Level Two: Mostly aligned with the intent of the mitigation strategy.
* Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

The baseline level of protection is achieved once an organisation is aligned at maturity level three for all the eight mitigation strategies. This is precisely defined by the ASCS as an explicit list of behaviours and standards. Where the risk is identified as higher for a given organisation, specialised advice may be provided to develop maturity beyond maturity level three. (Australian Cyber Security Centre, 2020)

### 1.1.3 ASD Essential Eight Mitigation Maturity Model Toolkit Product Tribe

The ASD Essential Eight forms the baseline of the proposed product; Cyber Security Capability and Maturity Consultancy Services, SecureBiz. The aim of this proposal is to “Research, assess and determine key applications of the Australian Signals Directorate (ASD) Essential Eight mitigation strategies in the small to medium enterprise business environment.” (Mcmeikan, 2019)

In Phase 1, the intent is to research, assess, design and develop tools, processes and documentation to be used by Deakin’s Australian Cyber Protection Centre consultancy division (DACPC) as part of a new business venture. These resources are the supporting foundations of the Deakin University Student Cyber Security Consultancy, which will deliver assessments and security advice to small-to-medium enterprises.

The format of the requested output is a product which meets the above needs. It should be an effective tool to support determining a business’s current risk profile, and then additionally testing and evaluating the implementation based on the Essential Eight Maturity Model.

## 1.2 Major Purpose of Document

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.

### 1.2.1 Management of this document

This document references specific features of the product under development subjected to change over time. This document, therefore, should be upkept with the relevant system changes introduced each sprint. Changes, including additions and modifications to this document should be tracked by a log in the table 0.1: Contributors.

# System Overview

The SecureBiz platform contains the following major components:

1. The “Get Started” button
2. Mitigation Strategy Breakdown and Analysis
3. The Feedback form
4. Admin Console



1.

2.

4.

3.

Figure 1: The landing page

## 2.1 The “Get Started” Questionnaire

When the user first accesses the web application, they are presented with a prominent button labelled “Get Started” on the left panel of the screen. When the user selects this button, a survey launches which iterates through a specific subset of questions for each of the mitigation strategies. At the end of the survey, a short report is produced which describes the outcome of the survey including the maturity level reached for each of the mitigation strategies.

Detail about this questionnaire can be found in section 3.2.

## 2.2 Mitigation Strategy Breakdown and Analysis

The “Assess” option in the top-of-page toolbar contains a clickable list of each of the eight mitigation strategies. Selection of one of these mitigation strategies launches a survey which iterates through all the questions related to that mitigation strategy. At the end of the survey, a short report is produced which describes the outcome of the survey including the maturity level reached for that mitigation strategy, and recommendations to improve related areas of the client’s security posture.



Figure 2: The Mitigation Strategies Questionnaire access via the ‘Assess’ link

Detail about this questionnaire can be found in section 3.3.

## 2.3 Feedback form

The feedback form appears as a pop-up when the user selects the Feedback button on the front page. It consists of a text field and a submit button, which provides the user an option to give feedback to the consultant/developers. This functionality is in progress and the responses are not yet configured to be received in the back end.



Figure 3: User Feedback form

## 2.4 Admin Console

The admin console is a consultant-side tool built into the User Interface (UI), which allows modification, addition and deletion of the questions which are used for the assessment and analysis of the client’s security posture. It also contains options to see management information and paradata associated with the data collected across all clients, which can be used to include further improvements to the system.

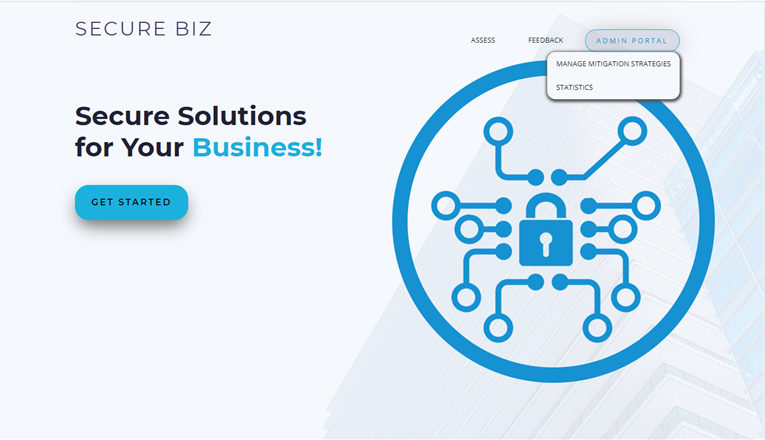


Figure 4: Admin Console access via the ‘Admin Console’ link

The admin console is further discussed in section 6.

# Maturity Assessment

## Overview

A questionnaire was chosen as the approach applied in the SecureBiz product, to determine the current state security posture of a client. The benefits of this is that it is simple to configure and only relies upon the experience of the client; so it can be seamlessly applied to any sized business of any purpose, using any range of devices or operating systems.

The questionnaire sits within the SecureBiz product, accessible via the Assess or Get Started links. The current expected use case is intended to be on a device in the hand of the consultant, who will collaborate with the client to respond to each of the questions by presenting them in turn and selecting a response as appropriate. The questionnaire is designed to structure the conversation between the consultant and the client; to quickly and succinctly obtain all the information about the current security measures in place in the client’s systems. There are multiple points of initialisation and configurations of questions, which may be used at different times depending upon the client’s needs, but all of them consist of presenting the client with a pop-up box as in the figure below (Figure 6).

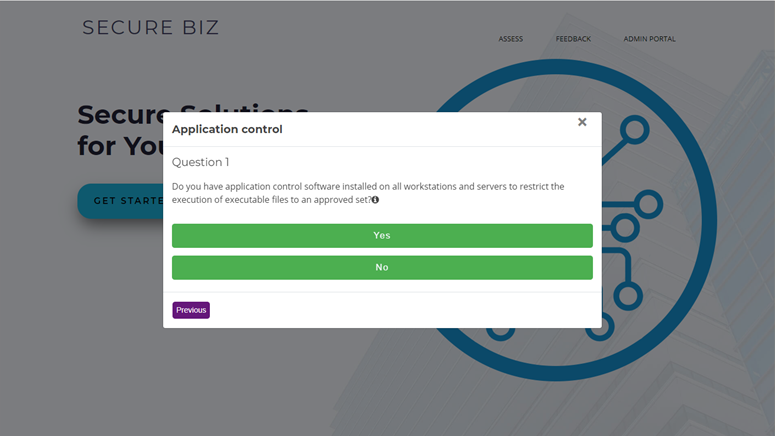


Figure 5: The question pop-up

The respondent moves through the questionnaire by selecting a response to the question. All question responses are closed, with a majority being of a “Yes” or “No” type. The respondent can change a response given to the previous question by selecting the ‘previous’ hyperlink, and will be required to resubmit a response to move forward again. If selecting ‘previous’ on the first question of the set, the questionnaire window disappears and will need to be reinitiated to be completed.

For select questions, additional detail can be provided if the respondent needs further information in order to respond to the question. This information can be viewed by mouse-hovering over the question mark icon at the end of the question, which causes a text bubble to appear with additional information (Figure 3.2).

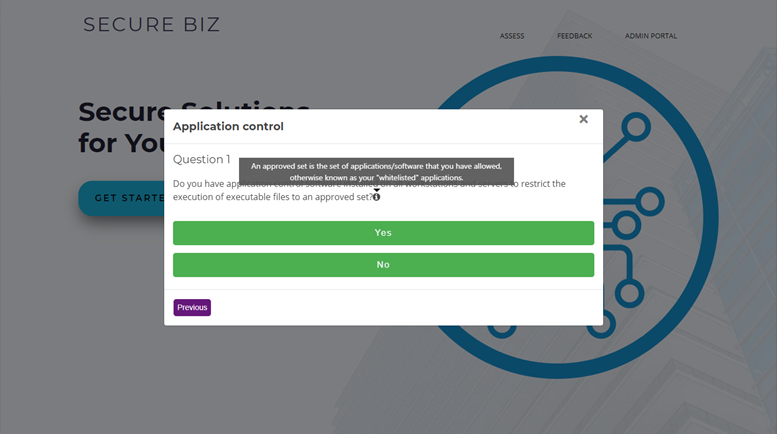


Figure 6: The question pop-up, with mouse over hover.

At the conclusion of the questionnaire, the respondent is provided with a congratulatory message, and maturity level report data is shown on screen alongside the number of questions completed and the mitigation strategy (Figure 7). Two buttons are also available to view the client report as a PDF or HTML.

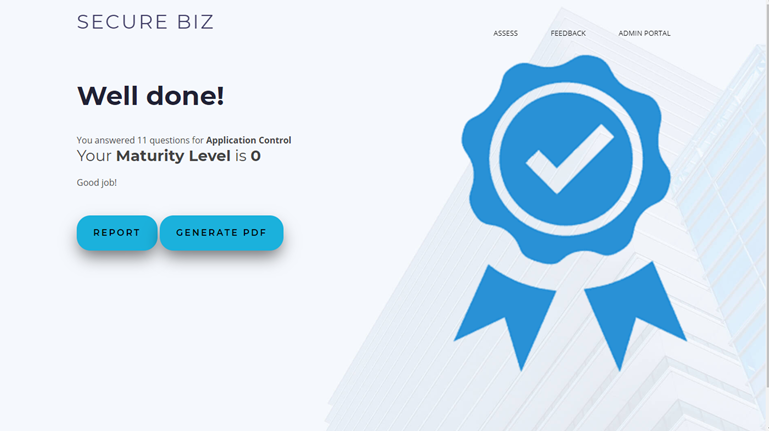


Figure 7: End of questionnaire message

Further information on the user interface can be found [here](https://teams.microsoft.com/l/file/CAC0E052-5666-4770-9783-01C29E839385?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%2FHandover%20Artefacts%2FFront-end%20and%20Back-end%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) (Front-end and Back-end Documentation).

Get Started works the same way, but instead of base then extended, it consists of each of the base question sets of all mitigation strategies in order.

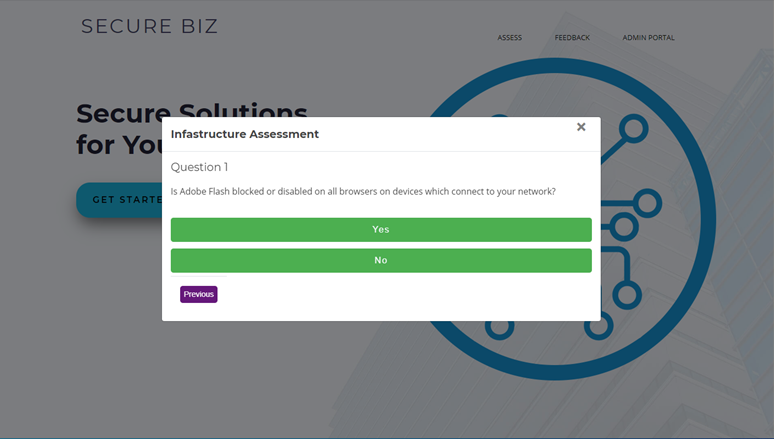


Figure 8: Get Started Questions

Additionally, the end of questionnaire for the ‘Get Started’ questionnaire concludes with a table consisting of each mitigation strategy listed by name and the achieved maturity level (Figure 9). Two buttons are also available to view the client report as a PDF or HTML.

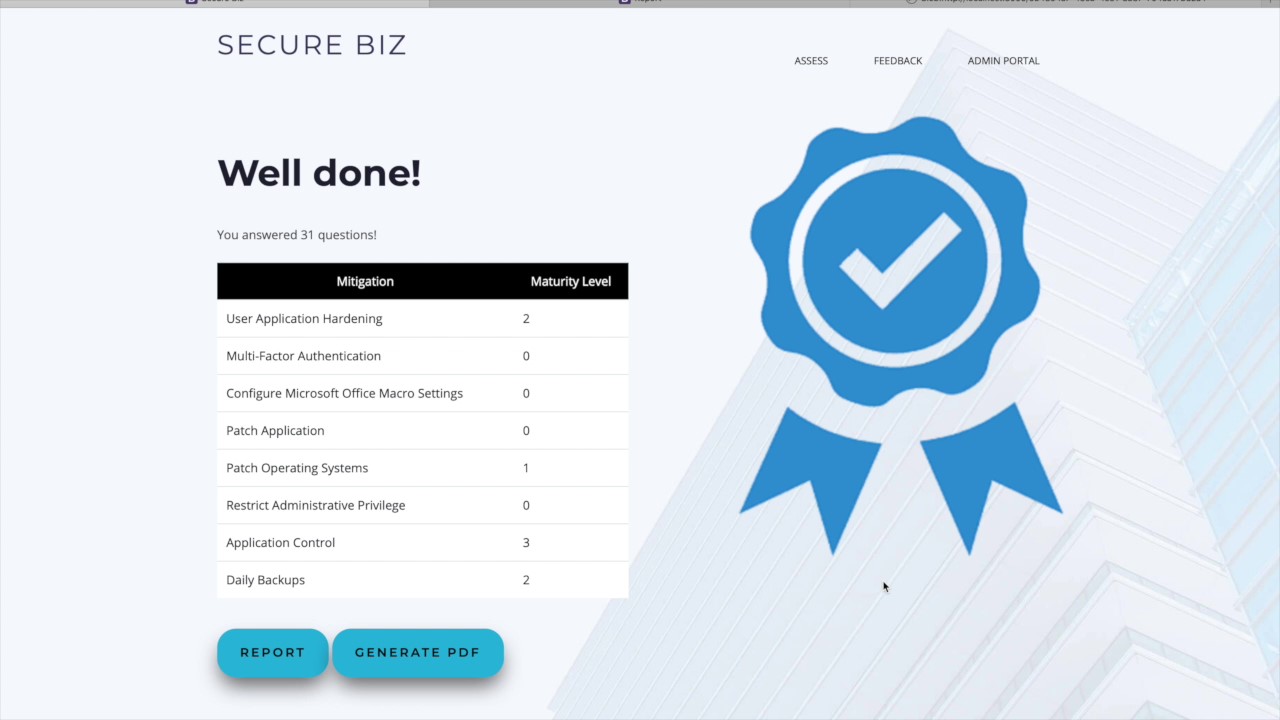


Figure 9: Get Started end of questionnaire message

## The Questionnaire Structure

The interview questions have been split into two functional groups; base and extended. The base questions directly respond to the standards set out in the ASD Essential Eight and represent a minimum coverage of the subject matter for each mitigation strategy within. The extended questions for each mitigation strategy extend the concepts covered in the baseline and broaden the review of the clients’ reception of the mitigation strategy.

The two-tiered approach was used to ensure the resulting product was flexible to the use-case of the client, and the level of detail used matched what was needed. The user will be required to cover the whole of the base questions for all eight mitigation strategies in order to fully assess their maturity for these in regards to the intentions of ASD Essential Eight; which is to ensure a minimum security maturity level is reached across the eight focus areas.

For each question, the following components are defined:

* **Question ID**  
  The Question ID is the mitigation strategy it belongs to, in short or long notation, followed by the number dictating its position within the questionnaire associated with that mitigation strategy. For clarity, long notation (the full mitigation strategy) has been used in the tables and diagrams below. The question numbers continue iteratively for the extended question sets.   
  i.e. The first question for the Application Control mitigation strategy is *Application Control Q1* or *AC1*. The first extended question is the fourth question and would therefore be the *Application Control Q4* or *AC4*.
* **Question Text**  
  The question itself, in the wording that is provided to the respondent.
* **Additional Detail**  
  Any information required to interpret the question is provided in the additional detail field, which populates a hover button on the question in the product.
* **Responses**  
  Provided as a list within the table cell, these are the responses which are available to the respondent for the given question.

The question logic flow is provided in the subsequent diagram.

### Use Cases

#### Get Started

If the respondent were to select the *Get Started* option on the front page, they would be presented with each of the questions of the base questionnaires, for each mitigation strategy in turn. The questions are provided with all questions of the mitigation strategy presented in turn before moving on to subsequent strategies, and the client’s maturity level for each mitigation strategy, in turn, will be calculated and presented in the final report.

The use case for this questionnaire is for performing the initial assessment of the user’s maturity level. It provides a streamline route to a clear assessment of maturity with little additional detail and no expansion, covering the full breadth of the Essential Eight at once. This would be the starting point for the user, providing information as to which areas are requiring more focus than others, and setting the user up to efficiently address their security vulnerabilities. If the user was to have a maturity level 3 outcome on any of the mitigation strategies, they would then know that further attention is not required, and would not need to complete the assess survey of this mitigation strategy.

#### Assess

If the respondent were to select any of the mitigation strategies listed under the *Assess* option on the front page, they would be presented with all the questions, base and extended, for that mitigation strategy, in turn. The base questions are presented first, and the extended questions follow, expanding on the topics and considerations touched on in the baseline. The client’s maturity level in relation to this mitigation strategy would be calculated from these responses, in addition to a comprehensive set of advice to improve the security standing of their cyber infrastructure in the form of a report.

The use case for this questionnaire is for performing an in-depth assessment of the client’s security posture in regards to one specific area; prompted by a low maturity level in the initial assessment, client special interest or concern, or systematic in-depth profiling of the system.

### Considerations

The following is a list of considerations recommended for questionnaire or survey building, and a response which describes the current state of the questionnaire regarding these considerations. This resource may be consulted to further enhance the quality of the questionnaire.

#### 3.2.2.1 Bias

Question phrasing may introduce bias that leans a respondent towards a desirable answer. Where possible, this bias should be reduced; excluding statements with imbedded opinions which may sway the respondent from answering accurately (Fisher, 2020). Loaded questions and leading words also contribute to this bias (Lloyd, 2018; Survey Monkey, 2020; Harrison, 2007).

This questionnaire is not intended primarily for market research, but rather to dictate a client’s adherence to a desired set of principles, which puts discussions of introduction of bias in a different light. The questions which are asked surround specific areas of security weakness and intrinsically have a preferential response. The current state of the questions has determined to avoid emotive or descriptive language in lieu of precise statements, however, relies upon the diligence of the respondent to answer accurately and leaves some element of bias-management burden on them.

#### 3.2.2.2 Jargon

The language used in the questionnaire should be easily accessible for the user; only as complex and detailed as necessary (Harrison, 2007). Language and terminology used should be that which the user is able to understand, and jargon should be avoided (Fisher, 2020; Lloyd, 2018; Harrison, 2007).

Care has been taken to ensure accessibility and usability of the language of the questions, to cater to a broad range of users. Where possible, questions have been phrased in common language. Where complex concepts are covered and unable to succinctly be converted to natural language, additional detail which includes simple and explicit descriptions can be easily accessed via a hover button on the interface.

#### 3.2.2.3 Exhaustive listings

Multiple choice questions should cover every possible response, allowing for an accurate response to each question (Lloyd, 2018; Harrison, 2007). The user should not need to have to put effort in to decide which response is the closest; the edges should be clearly defined with no overlap and no missed responses, and questions phrased to support this (Lloyd, 2018).

The majority of questions effectively address the full breadth of possible responses, with some exceptions which have been raised during User Acceptance Testing (UAT). Responses are intended to be revised to meet this standard in order to meet minimum viable product (MVP).

#### 3.2.2.4 Mandatory responses

Questions should not be mandatory, users should be given the option not to respond (Lloyd, 2018).

In current state, functionality has not been built to skip questions or to end the questionnaire prematurely, therefore questions are functionally equivalent to mandatory once the survey is initiated. This will be addressed for MVP.

#### 3.2.2.5 Specificity

Questions should be direct and specific, using clear and precise language facilitates ease in response (Fisher, 2020; Lloyd, 2018; Harrison, 2007). Questions should be asked one at a time, on a single and specific concept (Fisher, 2020; Lloyd, 2018; Survey Monkey, 2020; Harrison, 2007).

For a majority of questions, this requirement has been met. Exceptions have been raised in UAT and will be revised.

#### 3.2.2.6 Precision

The questionnaire should have a clearly articulated goal (Survey Monkey, 2020), for which each question in the questionnaire should be directly useful for achieving (Fisher, 2020). The survey should be kept as short and simple as possible while covering the breadth of the issue, as this ensures more thoughtful responses for the questions which were asked (Fisher, 2020; Field, 2003; Harrison, 2007).

The questionnaire purpose has been clearly articulated as part of this document. Questions have been reviewed to ensure within a single mitigation strategy, there is no redundancy to the questions, and solution to address broader redundancies is currently in the backlog.

Each question has a defined purpose; base questions for calculation of the maturity level and extended questions to determine the necessity of individual implementation advice segments which are provided to the user upon completion.

#### 3.2.2.7 Response Types

Open questions and grid or matrix questions introduce additional burden on the respondent and should be avoided (Fisher, 2020), but close-ended questions allow the user to align themselves with supplied positions, therefore reducing this burden (Survey Monkey, 2020), however this does, in turn, increase the opportunities for biased response scales. Closed-ended questions also reduce the variability in how the question can be interpreted, which can streamline responses (Harrison, 2007).

Where possible, yes/no responses should be avoided as they do not provide a rich response option for questions which may not be clear-cut (Fisher, 2020). Where scales are used, they should be balanced; only an extreme case requisite of an scale-edge response, a mediocre case requisite of a middle-ground response; in order to avoid swaying the user in any direction along the scale (Fisher, 2020). Yes/No scales can be risky if the response is not clear, user may be biased towards the desirable answer, therefore reducing the quality of the response data (Field, 2003).

The responses for these questions are primarily in yes/no format to match the statement format as noted in 3.2.2.1, with some other short-list response types for specific questions. This is required to be functional with the logic in the back end, as questions responses are matched one-to-one with a report action. Flexibility in this will not be part of MVP.

#### 3.2.2.8 Question order

Simple questions and high priority questions should be asked first, to avoid negative impact of respondent fatigue. More complex or sensitive questions should be asked towards the end (Fisher, 2020). Questions should be asked in a logical order which follows a conversational and context flow, level of specificity layered with progress (Lloyd, 2018). Additionally, questions should not be asked if they are not relevant to the user (Harrison, 2007).

All questionnaires follow a single static question order; for assess questionnaires this involves base questions appearing first. Care has been taken to ensure logical flow of the questions, including questions with depth (a parent-child question pair for which a response to the parent may negate relevance of the child); which are facilitated by appearing after their parent question with a *question is not relevant* response option so that they can be skipped.

## The Essential Eight

### 3.3.1 Application Control

#### 3.3.1.1 Overview

Application control is a security approach designed to protect against malicious code and software, malware, executing on systems. When implemented properly it ensures that only approved applications, such as executables, software libraries, scripts, and installers, can be executed.

While application control is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unapproved applications (Australian Cyber Security Centre, 2020).

Questions which determine the client’s security posture in regard to application control focus on core concepts such as:

* preventing unrecognised or undesirable applications and software from establishing themselves on the client’s devices
* verifying the authenticity of applications
* use of policy and appropriate use of admin privileges to reduce risk of overwriting preventions
* verifying risk prevention tactics remain in place
* using commercial software to improve the security of devices

#### 3.3.1.2 Assessment

The base questions of the application control mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Application Control Q1 | Do you have application control software installed on all workstations and servers to restrict the execution of executable files to an approved set? | An approved set is the set of applications/software that you have allowed, otherwise known as your “whitelisted” applications. | * Yes * No |
| Application Control Q2 | Does your application control software restrict the execution of software libraries, scripts and installers on all workstations and servers to an approved set? | An approved set is the set of applications/software that you have allowed, otherwise known as your “whitelisted” applications. | * Yes * No |
| Application Control Q3 | Have you implemented Microsoft’s latest block rules? |  | * Yes * No |

Table 1: Application Control base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 9.

A picture containing computer

Description automatically generated

Figure 9: Application Control maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

### 3.3.2 Patch Applications

#### 3.3.2.1 Overview

Application patches are revised code components and application versions which are updated and released by the vendor in response to issues found in earlier versions. Patches are commonly used to address security vulnerabilities found in applications, and their timely implementation is necessary in order to maintain the security of the user’s software. An application will have a lifespan during which the vendor may continue to monitor security risks and supply patches where vulnerabilities are identified. However, for most products, vendor support will eventually cease, at which point the security of the application is no longer ensured.

The security vulnerability associated with an application patch will be unique in applicability and importance, and the risk to the business will need to be determined for each in order to choose the correct course of action. Risk should be considered noting that the existence of a security patch implies the existence of a security vulnerability which can then easily and quickly identified by adversaries and exploited (Australian Cyber Security Centre, 2020).

Questions which determine the client’s security posture in regards to application patching focus on core concepts such as:

* response time
* capability to quickly identify risk and broadly implement patches
* appropriate policy for risk reduction
* up-to-date intel
* internal application security verification
* contingency plans

#### 3.3.2.2 Assessment

The base questions of the patch application mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Patch Applications Q1 | If a critical security vulnerability is identified, how quickly do you apply an appropriate patch or mitigation for the affected system or application? | This refers to patches and updates that address critical vulnerabilities and security exploits | 1. Within 48 hours 2. Within two weeks 3. Within one month 4. Longer than one month |
| Patch Applications Q2 | Do you replace systems and applications where the vendor has ceased providing patches and updates? | Do you seek out replacement applications with similar functionality if an application loses support for new patches and security updates from the vendor? | * Yes * No |
| Patch Applications Q3 | Do you have an automated process that tracks and records the successful installation of patches and updates for applications? |  | * Yes * No |

Table 2: Patch Applications base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 10.

A close up of a logo

Description automatically generated

Figure 10: Patch Applications maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

### 3.3.3 Configure Microsoft Office macro settings

#### 3.3.3.1 Overview

A macro is a small program which can be imbedded within Microsoft office to perform a broad range of tasks and supply functionality, however, they are vulnerable to being used maliciously and if unregulated, pose a risk to the security of the user’s software and data.

Questions which determine the client’s security posture in regards to Microsoft Office macros focus on core concepts such as:

* ensuring prerequisites such as originating from trusted documents or trusted locations are met
* risky documents are not able to enter the client’s devices
* third parties are not able to execute macros on documents which are required to enter

#### 3.3.3.2 Assessment

The base questions of the Microsoft office macros mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Microsoft Office Macros Q1 | Please choose the most relevant answer for your current macro security setup: |  | 1. Microsoft Office macros are only allowed to execute from trusted locations where write access is locked down to administrators who appropriately evaluate macros before adding files into these locations 2. Only digitally signed Microsoft Office Macros from trusted publishers are allowed to execute 3. Microsoft Office macros are allowed to execute after user approval |
| Microsoft Office Macros Q2 | Are Microsoft Office macro settings configured so that end users cannot change settings? | - | * Yes * No |
| Microsoft Office Macros Q3 | Do you block Microsoft Office macros in documents that originate from the internet? |  | * Yes * No |

Table 3: Microsoft Office Macros base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 11.

A close up of a logo

Description automatically generated

Figure 11: Microsoft Office Macros maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

### 3.3.4 User Application Hardening

#### 3.3.4.1 Overview

Application hardening is the act of reducing the attack surfaces of applications by reducing functionality down to the minimums that are required, blocking common access points of malicious software and making it difficult for malicious software to move through the system once it gains access.

There are key applications which are represented in the ASD Essential Eight maturity model as being of the first priority to protect; web browsers and Microsoft Office. Web browsers present a large risk as they are the window through which to access the world wide web, which is wrought with cyber security risks. With its broad range of users and user intents, the web is a largely unregulated living mass of applications, sites, and files; a sizeable proportion of which are criminally inclined. Some web and application components, designed with the ease of the user in mind, can present as a portal through which to access your computer and implant malware or access sensitive information.

It is not usually possible to determine which components may contain malicious intent, so the approach of the ASD is to broadly disable these functionalities and harden the software against these common risks. Generally, these functionalities are those which imbed some an external application within the file or site accessed, the security of which is not assessed at the same or desired level of scrutiny (Australian Cyber Security Centre, 2020).

Questions which determine the client’s security posture in regards to application hardening focus on concepts such as:

* blocking or preventing the use of risky but unnecessary ‘nice to have’ imbedded applications and functionality
* logging and restricting points of access for malware

#### 3.3.4.2 Assessment

The base questions of the application hardening mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Application Hardening Q1 | Is Adobe Flash blocked or disabled on all browsers on devices which connect to your network? | - | * Yes * No |
| Application Hardening Q2 | Are web advertisements blocked on all browsers on devices which connect to your network? | - | * Yes * No |
| Application Hardening Q3 | Is Java from the internet blocked on all browsers on devices which connect to your network? | - | * Yes * No |
| Application Hardening Q4 | Is Microsoft Office or equivalent software blocked from using object linking and embedding on your devices? | Object Linking and Embedding (OLE) is technology created by Microsoft which enables drag and drop and clipboard functionality between applications, as well as the embedding (an independent copy) or linking (a live connection) of an application within another, such as an excel spreadsheet within a word document | * Yes * No |
| Application Hardening Q5 | Is Adobe Flash blocked in Microsoft Office or equivalent software on your devices? | - | * Yes * No |

Table 4: Application hardening base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 12.

A screenshot of a cell phone

Description automatically generated

Figure 12: Application Hardening maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

### 3.3.5 Restrict Administrative Privileges

#### 3.3.5.1 Overview

Administrative privileges are system roles which permit the user or application to access data, make system changes, bypass security settings and complete high-risk tasks that are not permitted of the average user. Where administrative privileges are restricted and regulated, malware which has penetrated the system will have greater barriers to overcome in order to access restricted data or make significant system changes, and system recovery after a breach is easier, as damage is less significant. Restriction of administrative privileges can also protect the client against internal risks, intentional or unintentional malicious activity executed by internal users (Australian Cyber Security Centre, 2019).

Questions which determine the client’s security posture in regard to administrative privileges focus on:

* ensuring that administrative privileges are required for high risk activities
* are only provided where they are necessary
* administrative accounts are monitored, verified, and vetted

#### Assessment

The base questions of the restrict administrative privileges mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Restrict Admin Privileges Q1 | Are requests for privileged access to systems, applications and information validated upon request? | - | * Yes * No |
| Restrict Admin Privileges Q2 | Are controls in place to prevent privileged and administrator users from accessing emails, browsing the web and obtaining files via online services? | - | * Yes * No |
| Restrict Admin Privileges Q3 | Is privileged access to systems, applications and information re-evaluated on an annual or better basis? | - | * Yes * No |
| Restrict Admin Privileges Q4 | Are privileged and/or administrative users only given the necessary privileges and access as required by their role(s)? | - | * Yes * No |

Table 5: Restrict administrative privileges base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 13.

A screenshot of a cell phone

Description automatically generated

Figure 13: Restrict Administrative Privileges maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

### 3.3.6 Patch Operating Systems

#### 3.3.6.1 Overview

Patching workstations, services and ICT equipment is important, much as patching of applications is important. Patches for security vulnerabilities in operating systems need to be implemented promptly, as the unpatched vulnerability can be used to compromise the system (Australian Cyber Security Centre, 2020).

It is essential that patching and risk mitigation for operating systems on computers and network devices with very high risk vulnerabilities are acted upon within 48 hours, and that only the latest and supported operating system versions are in use (Australian Cyber Security Centre, 2017).

Questions which determine the client’s security posture in regard to patching operating systems, focus on key concepts such as:

* rapid identification and classification of urgency of patches
* appropriate policy for risk reduction
* up-to-date intel
* internal application security verification
* contingency plans

#### 3.3.6.2 Assessment

The base questions of the patch operating systems mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Patch Operating Systems Q1 | When a security vulnerability is identified by a vendor or system manager as a critical risk, when is the vulnerability patched? | This refers to patches and updates that address critical vulnerabilities and security exploits. A patch refers to a fix provided by a vendor or third party which repairs or covers a security flaw | 1. Within 48 hours 2. Within two weeks 3. Within one month 4. Longer than one month |
| Patch Operating Systems Q2 | Do you replace all operating systems for workstations, servers or ICT equipment that no longer receive updates or patches from the vendor? | Do you seek out replacement operating systems with similar functionality if an operating system loses support for new patches and security updates from the vendor? | * Yes * No |
| Patch Operating Systems Q3 | Do you have an automated process that tracks and records the successful installation of patches and updates for operation systems? | - | * Yes * No |

Table 6: Patch operating systems base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 14.

A picture containing computer

Description automatically generated

Figure 14: Patch operating systems maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

### 3.3.7 Multi-Factor Authentication

#### 3.3.7.1 Overview

Multi-factor authentication is a powerful tool for preventing unauthorised access or use of a device or access to a network. The principle follows that an adversary may gain access to a system authenticated by a single factor via obtaining a user’s credentials, but that the likelihood of gaining access is significantly reduced when multiple authentication factors are used and are required to match. A system has implemented multi-factor authentication when a single user is required to produce two or more separate factors to authenticate their identity, before system access is granted. These factors may be any combination of physical or software object, a piece of personal information, or bio identifier (Australian Cyber Security Centre, 2019).

Questions which determine the client’s security posture in regard to authentication practices focus on:

* ensuring that multi-factor authentication is used to protect important assets
* that its use is effective in that the authentication methods themselves are distinct, mandatory, and protected.

#### 3.3.7.2 Assessment

The base questions of the multi-factor authentication mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Multi-Factor Authentication Q1 | Does the business use Multi-Factor Authentication to authenticate all users for remote access solutions? | - | * Yes * No |
| Multi-Factor Authentication Q2 | Multi-factor authentication uses at least two of the following authentication factors: | - | * Yes * No |
| Multi-Factor Authentication Q3 | Is MFA used to authenticate all privileged users and any other positions of trust? | - | 1. Password with 6 or more characters (10) 2. Universal 2nd Factor Security Key (10) 3. Smartcards (10) 4. Physical one-time password token 5. Biometrics (10) 6. SMS Messages (4) 7. Email (3) 8. Voice Call (2) 9. Software Certificate (1) 10. Mobile Application one-time password token (5) 11. None of the above (0) |
| Multi-Factor Authentication Q4 | Is MFA used to authenticate all users when accessing important data repositories? | - | * Yes * No |

Table 7: Multi-factor authentication base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 15.

Figure 15: Multi-Factor Authentication maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

### 3.3.8 Daily Backups

#### 3.3.8.1 Overview

System state and data backups are an essential requirement for system restoration after a breach, so that business can resume and continuity is protected in the case where the system or data was altered or compromised. Backups cannot remove data from the hands of adversaries, but it can provide a stable, recent state for the system to return to, and function as an inventory of the content that may have been accessed as part of the incident.

Questions which determine the client’s security posture in regard to system and data backups focus on ensuring that backups are:

* made regularly of all appropriate system items and data
* stored appropriately
* fit for purpose

3.3.8.2 Assessment A close up of a logo

Description automatically generated

The base questions of the daily backups mitigation strategy are found in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Question ID** | **Question Text** | **Additional Detail** | **Question Responses** |
| Daily Backups Q1 | How often do you perform backups of important information, software and configuration settings? | - | 1. Daily 2. Weekly 3. Monthly 4. More than Monthly or not at all |
| Daily Backups Q2 | How long do you store backups for? | - | 1. 3 months or greater 2. Between 1 and 3 months 3. Less than 1 month or not at all |
| Daily Backups Q3 | How often do you test partial restoration of backups? | - | 1. Quarterly or better 2. Bi-annually or better 3. Annually or better 4. No partial test completed |
| Daily Backups Q4 | Do you test full restoration of backups at least once? | - | * Yes * No |
| Daily Backups Q5 | Do you store backups either offline, or online but in a non-rewritable and non-erasable manner? | - | * Yes * No |
| Daily Backups Q6 | Do you test full restoration of backups each time fundamental information technology infrastructure changes occur? | In this instance, infrastructure changes can include major patches/updates, new physical infrastructure being introduced or new systems/software/ applications being installed and configured. | * Yes * No |

Table 8: Daily backups base questions

The maturity level of the client is then determined from the responses provided to these questions, according to figure 16.

A close up of electronics

Description automatically generated

Figure 16: Daily Backups maturity determination logic

For each maturity level shy of maturity 3, advice is supplied in the client report to support the user in implementing changes to meet the baseline goal of maturity level 3.

## Extension

Extension questions were produced for each mitigation strategy to widen the reach of the questionnaire and provide broader and better-established advice for improving their maturity posture. Questions for each mitigation strategy were conceived by consulting sources such as the American National Institute of Standards and Technology (NIST) and ACSC.

The extension questions are not static, as they are configurable via the admin panel. As a result, they are not included within this document.

These questions can be found within the Question Change Log. Please see section 4: *Making Changes to the Questions* and appendix 8.4: *Change Management* for further detail.

# Making Changes to the Questions

The admin console makes it possible for the user to make changes to the questions in the database, including adding and removing questions, from the front end. Question changes and versions are not currently stored in the system, and there is no built-in way to track this, so a business process has been put in place to ensure business continuity.

## Question Change Log

The question change log is an excel spreadsheet which is used to track any changes made to the questions via business process. The spreadsheet contains two sheets, the first with a log of all questions and changes made to the questions, and the second with validation lists used to restrict the data in the first.

The change log tab contains all the information about the questions which are expected to be present in the system and the history of the changes which have occurred. It can be used to track and restore the questions if unauthorised changes were made through the admin console and provides a neat overview of all the questions in the system so that they may be reviewed.

The headings consist of all the information about the questions which is required for them to be added or edited, including flags for question edits or question deletion. It also contains fields to record a sign-off and implementation process, including justification of the change. Excel validation logic has been applied to some of these fields to restrict the entries to valid responses; where this has occurred, it has been described in the right column.

|  |  |
| --- | --- |
| Current Flag | *A manual Flag for triggering whether the row corresponds to the most recent change. Restricted to values yes/no* |
| Date of Update | *The date this question was updated/added* |
| New Question Flag | *Is this an update to an existing question, or a new question?**Restricted to values yes/no* |
| Question Deletion Flag | *Is this a deletion of an existing question?**Restricted to values yes/no* |
| Duplicate Flag | *Is this question represented across multiple mitigation strategies?**Restricted to values yes/no* |
| Mitigation Strategy | *Which collection set does this question belong to? Restricted to values AC, PA, OMS, AH, RAP, POS, MFA, DA* |
| Question Set | *Is this question a base or an extended question? Restricted to values base, extended* |
| Question Number | *What is the unique position of this question within the survey?* |
| Question | *The question itself, as it will be displayed to the client and consultant in the questionnaire* |
| Answers | *List of possible responses which the respondent may select when answering the question* |
| Additional Detail | *Further information about the question, which will appear under a '?' icon on the question screen, to provide specific information to the client about complex or technical questions* |
| Response Logic | *Which response triggers the mitigation strategy suggestion* |
| Mitigation Strategy Response | *The information displayed for a negative response in the report for the user.* |
| Editor | *The identity of the person who prepared the edit* |
| Reason for Edit | *The purpose for making the edit to the question* |
| Edit Secondary | *The identity of the person who reviewed and signed off the edit* |
| Edit Secondary date | *The date of the review and sign-off of the edit* |
| Implementary | *The identity of the person who implemented the change in the system* |
| Implementary date | *The date of the implementation of the change in the system* |
| Implementary Secondary | *The identity of the person who reviewed and tested the implementation* |
| Implementary Secondary date | *The date of the review and test of the implementation of the change in the system* |

Table 9: The Change Log column headings and column heading explanations

## Use of Question Change Log

### Adding a Question

Note: It is currently only possible for a user to add a question to the ‘extended’ question set for a given mitigation strategy via the admin console. Additions to the ‘base’ question set requires back-end editing of the maturity level calculation and is therefore outside of the scope of this business process.

Further note: The Change Log represents a live project component which is subject to change in future iterations, and as such these processes are also subject to change. They have been explicitly articulated below to support a minimum viable product ensuring the questions can be versioned responsibly.

1. Open the **Question Change Log** excel spreadsheet inside Microsoft Teams and select ‘Edit’
2. Open the **Change Log** tab
3. Scroll past all populated rows to the next fully empty column. Ensure the column is completely empty before making any changes, to avoid overwriting an earlier entry.
4. Enter “Yes” from the drop-down for the **Current Flag** field.
5. Enter the current date in the **Date of Update** field, in clear DD Mon YYYY format.
6. Select “Yes” from the drop-down in the **New Question Flag** field.
7. Select the relevant mitigation strategy (provided as an acronym) from the drop-down in the **Mitigation Strategy** field.
8. Select “extended” from the drop-down in the **Question Set** field
9. Enter the question number, which will be the next number in sequence after the current last question number for that question set/mitigation strategy, in the **Question Number** field.
10. Provide the Question text as required to be displayed in the **Question** Field.
11. Provide the answers, in the order you would like them to appear, in the **Answers** field, separated by a forward slash.
12. If required, supply any information which should be displayed under the additional detail hover in the **Additional Detail** field.
13. In the **Response Logic** field, specify which answer corresponds with the negative response and therefore should trigger a mitigation strategy in the report. This field is not validated, so supply sufficient information that the person who will implement the question is able to understand clearly.
14. In the **Mitigation Strategy Responses** field, provide the summary response that the user will receive when they respond negatively to the question, to be included in the report.
15. If the question exists elsewhere in another collection, select “Yes” from the drop-down in the **Duplicate Flag** field.
16. Provide your own name in the **Editor** field.
17. Provide a succinct description of the reason for the addition of the question in the **Reason for Edit** field.
18. Save the file.

The addition to the file will then need to be reviewed.

1. A secondary reviewer should access the file, and verify the content as entered above is correct.
2. The secondary reviewer is to supply their name to the **Edit Secondary** field as sign-off.
3. The secondary reviewer is to supply the date of review to the question to the Edit Secondary date field.

The addition to the product via the admin panel will then need to be actioned, and verified.

1. The implementary should access the file and use the information contained to add the question to the product via the admin panel.
2. The implementary is to supply their name to the **Implementary field** when actioned.
3. The implementary is to supply the date of implementation to the **Implementary date** field.
4. A secondary implementary should then access the file and access the product, and verify the question has been successfully added to the product and functions as expected.
5. The secondary implementary is to supply their name to the **Implementary Secondary** field when actioned.
6. The secondary implementary is to supply the date of verification to the **Implementary Secondary date** field.

If at any time the question is known to be incorrect:

* If this is noted prior to implementation, the issue should be raised with the Editor, who will need to make a change to the record including clearing the **Edit Secondary** and **Edit Secondary date** fields and re-initiate review.
* If it is noted post implementation, the issue should be raised as a new log, as a question edit. The review and verification process may be discarded if it is not complete, although if this is complete it is not necessary to remove the record.
* **DO NOT DELETE ANY LOG ITEMS**

### Editing a Question

Note: It is currently only possible for a user to edit superficial fields for a ‘base’ question, as to not impact maturity determination, via the admin panel. More significant edits to the ‘base’ question set requires back-end editing of the maturity level calculation and is therefore outside of the scope of this business process.

1. Open the **Question Change Log** excel spreadsheet inside Microsoft Teams and select ‘Edit’
2. Open the **Change Log** tab
3. Filter the **Current Flag** field by “Yes” and locate the question to be changed.
4. If the change is minor, the user may want to copy fields E to M to clipboard at this point.
5. Alter the value of the **Current Flag** field to “No” for this question, and then clear the filter.
6. Scroll past all populated rows to the next fully empty column. Ensure the column is completely empty before making any changes, to avoid overwriting an earlier entry.
7. Enter “Yes” from the drop-down for the **Current Flag** field.
8. Enter the current date in the **Date of Update** field, in clear DD Mon YYYY format.
9. Select “No” from the drop-down in the **New Question Flag** field.
10. Select “No” from the drop-down in the **Question Deletion Flag** field.
11. If the change is minor and the user copied the fields to clipboard, they may wish to paste them into fields E to M in this record to auto-populate to match the discarded question. If this is taken, the user should make the change required and proceed to the review stage, ensuring all fields are appropriately populated. If further detail is required of the user did not copy the fields, they should proceed through the following steps.
12. Select the relevant mitigation strategy (provided as an acronym) from the drop-down in the **Mitigation Strategy** field.
13. Select “extended” or “base” as required from the drop-down in the **Question Set** field
14. Enter the question number, which should match the question which was removed, in the **Question Number** field.
15. Provide the Question text as required to be displayed in the **Question** Field.
16. Provide the answers, in the order you would like them to appear, in the **Answers** field, separated by a forward slash.
17. If required, supply any information which should be displayed under the additional detail hover in the **Additional Detail** field.
18. In the **Response Logic** field, specify which answer corresponds with the negative response and therefore should trigger a mitigation strategy in the report. This field is not validated, so supply sufficient information that the person who will implement the question is able to understand clearly.
19. In the **Mitigation Strategy Responses** field, provide the summary response that the user will receive when they respond negatively to the question, to be included in the report.
20. If the question exists elsewhere in another collection, select “Yes” from the drop-down in the **Duplicate Flag** field.
21. Provide your own name in the **Editor** field.
22. Provide a succinct description of the reason for the addition of the question in the **Reason for Edit** field.
23. Save the file.

The alteration to the question will then need to be reviewed.

1. A secondary reviewer should access the file, and verify the content as entered above is correct.
2. The secondary reviewer is to supply their name to the **Edit Secondary** field as sign-off.
3. The secondary reviewer is to supply the date of review to the question to the Edit Secondary date field.

The alteration to the product via the admin panel will then need to be actioned, and verified.

1. The implementary should access the file and use the information contained to add the question to the product via the admin panel.
2. The implementary is to supply their name to the **Implementary field** when actioned.
3. The implementary is to supply the date of implementation to the **Implementary date** field.
4. A secondary implementary should then access the file and access the product, and verify the question has been successfully added to the product and functions as expected.
5. The secondary implementary is to supply their name to the **Implementary Secondary** field when actioned.
6. The secondary implementary is to supply the date of verification to the **Implementary Secondary date** field.

If at any time the question is known to be incorrect:

* If this is noted prior to implementation, the issue should be raised with the Editor, who will need to make a change to the record including clearing the **Edit Secondary** and **Edit Secondary date** fields and re-initiate review.
* If it is noted post implementation, the issue should be raised as a new log, as a question edit. The review and verification process may be discarded if it is not complete, although if this is complete it is not necessary to remove the record.
* **DO NOT DELETE ANY LOG ITEMS**

### Deleting a Question

Note: It is currently only possible for a user delete ‘extended’ questions, as to not impact maturity determination.

1. Open the **Question Change Log** excel spreadsheet inside Microsoft Teams and select ‘Edit’
2. Open the **Change Log** tab
3. Filter the **Current Flag** field by “Yes” and locate the question to be changed.
4. Alter the value of the **Current Flag** field to “No” for this question, and then clear the filter.
5. Scroll past all populated rows to the next fully empty column. Ensure the column is completely empty before making any changes, to avoid overwriting an earlier entry.
6. Enter “Yes” from the drop-down for the **Current Flag** field.
7. Enter the current date in the **Date of Update** field, in clear DD Mon YYYY format.
8. Select “No” from the drop-down in the **New Question Flag** field.
9. Select “Yes” from the drop-down in the **Question Deletion Flag** field.
10. Select the relevant mitigation strategy (provided as an acronym) from the drop-down in the **Mitigation Strategy** field.
11. Select “extended” from the drop-down in the **Question Set** field
12. Enter the question number, which should match the question which was removed, in the **Question Number** field.
13. The following fields are not required: **Question, Answers, Additional Detail, Response Logic, Mitigation Strategy Response.**
14. Provide your own name in the **Editor** field.
15. Provide a succinct description of the reason for the addition of the question in the **Reason for Edit** field.

The deletion of the question may impact the question order of other questions in the mitigation strategy. Please see the important note below.

1. Save the file.

The alteration to the question will then need to be reviewed.

1. A secondary reviewer should access the file, and verify the content as entered above is correct.
2. The secondary reviewer is to supply their name to the **Edit Secondary** field as sign-off.
3. The secondary reviewer is to supply the date of review to the question to the Edit Secondary date field.

The alteration to the product via the admin panel will then need to be actioned, and verified.

1. The implementary should access the file and use the information contained to add the question to the product via the admin panel.
2. The implementary is to supply their name to the **Implementary field** when actioned.
3. The implementary is to supply the date of implementation to the **Implementary date** field.
4. A secondary implementary should then access the file and access the product, and verify the question has been successfully added to the product and functions as expected.
5. The secondary implementary is to supply their name to the **Implementary Secondary** field when actioned.
6. The secondary implementary is to supply the date of verification to the **Implementary Secondary date** field.

Important Note:

If the question to be deleted is **not** the final question in the mitigation strategy question set; that is, the **Question Number** is not the highest number for that **Mitigation Strategy**; the user will need to edit all questions which appear after this question, to alter their **Question Number** to be reduced by 1. That is, for all questions within the same **Mitigation Strategy,** where the **Question Number** is higher than that of the deleted question, they will need to be edited as per the edit process in 4.2.2: Editing a question, to systematically reduce their **Question Number** by 1.

If at any time the action is known to be incorrect:

* If this is noted prior to implementation, the issue should be raised with the Editor, who will need to make a change to the record including clearing the **Edit Secondary** and **Edit Secondary date** fields and re-initiate review.
* If it is noted post implementation, the issue should be raised as a new log, as a question edit. The review and verification process may be discarded if it is not complete, although if this is complete it is not necessary to remove the record.
* **DO NOT DELETE ANY LOG ITEMS**

# Reporting

At the conclusion of both the Assess and Get Started Questionnaires, a report is generated. This report includes the details of the maturity level obtained, number of questions answered, and a table consisting of the recommendations based on the responses provided.

## 5.1 Get Started

When the user completes the Get Started questionnaire, they receive a maturity level and the recommendations based on responses to the core questions, for each of the eight mitigation strategies. At this final page, the user may choose to view the report as a PDF or as a HTML file.

### PDF Report

The PDF report will open in a new tab, with a file name that is a long randomised string. This file can then be saved from the browser as a PDF. The file itself consists of minimal visuals, including the ASD Essential Eight title, with ‘Presented by Securebiz’ emphasis, and a subsections of ‘Report Outline’ and ‘ASD Essential Eight Mitigation Strategy Results’ (Figure 18).

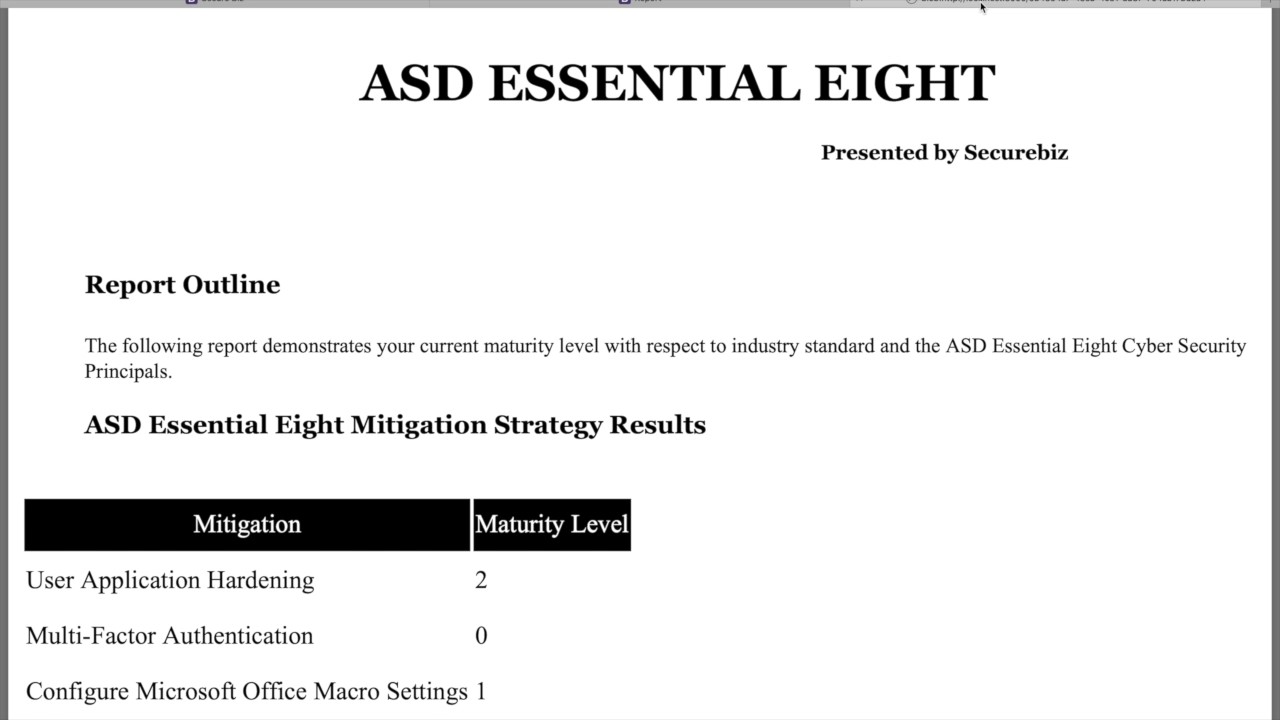


Figure 18: Get Started PDF report

The report outline contains a brief statement, followed by the results presented as a table similar to that shown on the front page at completion of the questionnaire, as discussed in section 3.1. The table contains a column of mitigation strategies listed by name, and a column with the calculated maturity level for each provided to the user.

Following this table is a second table containing the recommendations. This table has the headings of Question, Response and Mitigation; containing the question number, the text response as was selected by the respondent, followed by the paragraph of recommendations provided that explain why that response should be rectified.

### HTML Report

The HTML report will open in a new tab, with a file name that is a long, randomised string of alpha numeric characters. This file can then be saved from the browser as a PDF. The file itself consists of simple visuals aligned with the website itself. The text includes the ASD Essential Eight title, with ‘Presented by Securebiz’ emphasis, and the heading ‘Report Outline’, although the tables following are not titled.

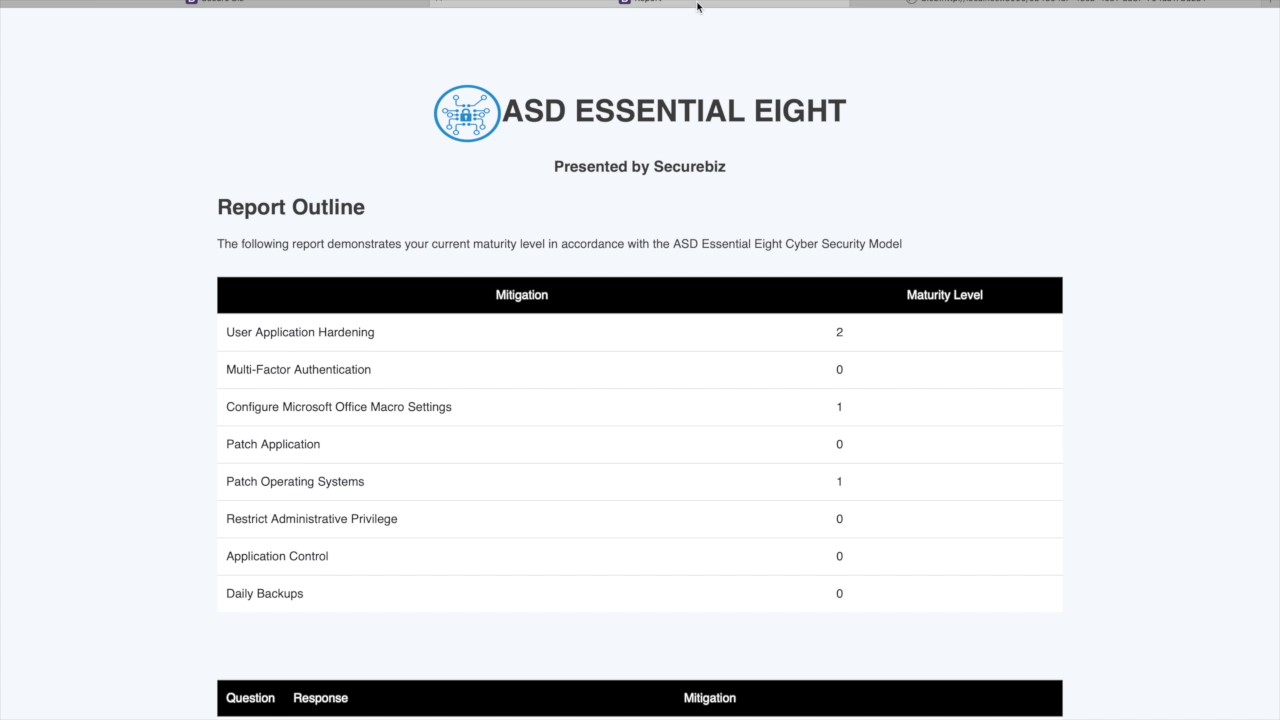


Figure 19: Get Started HTML report

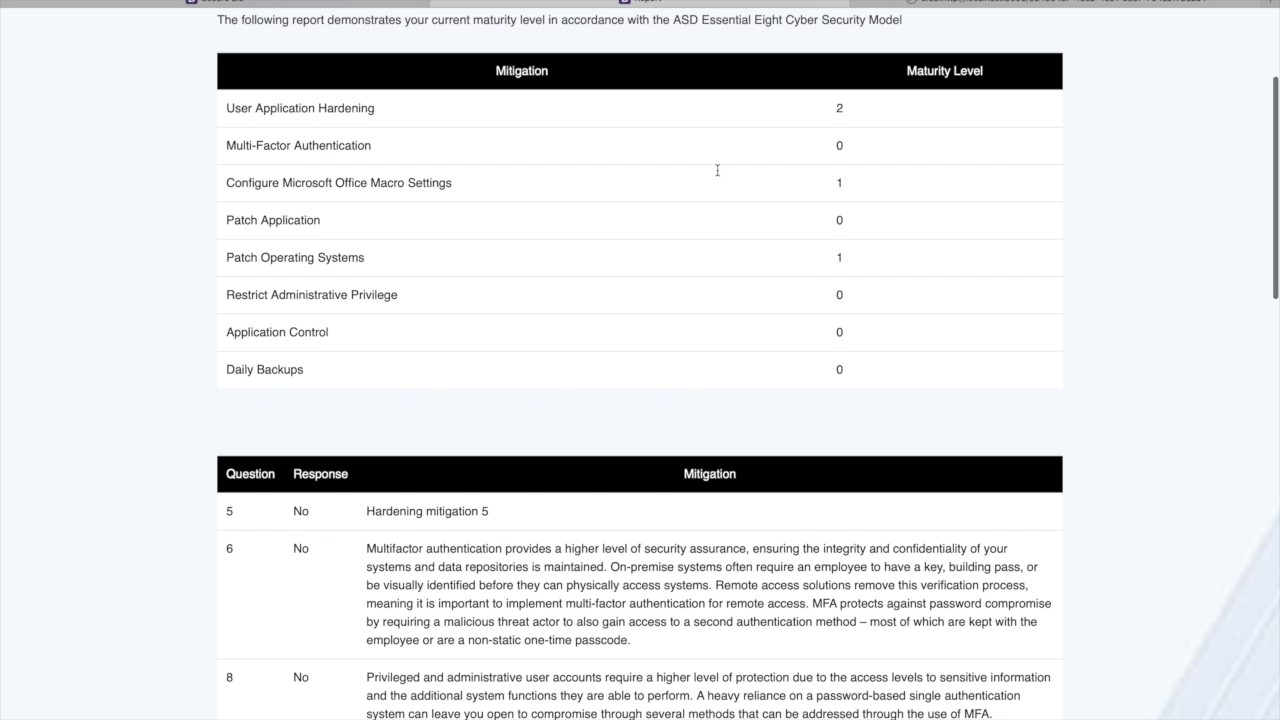


Figure 20: Get Started HTML report continued

As in the PDF, the report outline contains a brief statement, followed by the results presented as a table similar to that shown on the front page at completion of the questionnaire, as discussed in section 3.1. The table contains a column of mitigation strategies listed by name, and a column with the calculated maturity level for each provided to the user.

Following this table is a second table containing the recommendations. This table has the headings of Question, Response and Mitigation; containing the question number, the text response as was selected by the respondent, followed by the paragraph of recommendations provided that explain why that response should be rectified.

## 5.2 Assess

When the user completes any Assess questionnaire, they receive a maturity level for just that mitigation strategy and the recommendations based on responses to the base and extended questions. At this final page, the user may choose to view the report as a PDF or as a HTML file.

### PDF Report

The PDF report will open in a new tab, with a file name that is a long randomised string. This file can then be saved from the browser as a PDF. The file itself consists of minimal visuals, including the ASD Essential Eight title, with ‘Presented by Securebiz’ emphasis, and a subsections of ‘[Mitigation Strategy] - Report Outline’ and ‘ASD Essential Eight Mitigation Strategy Results’ (Figure 21).

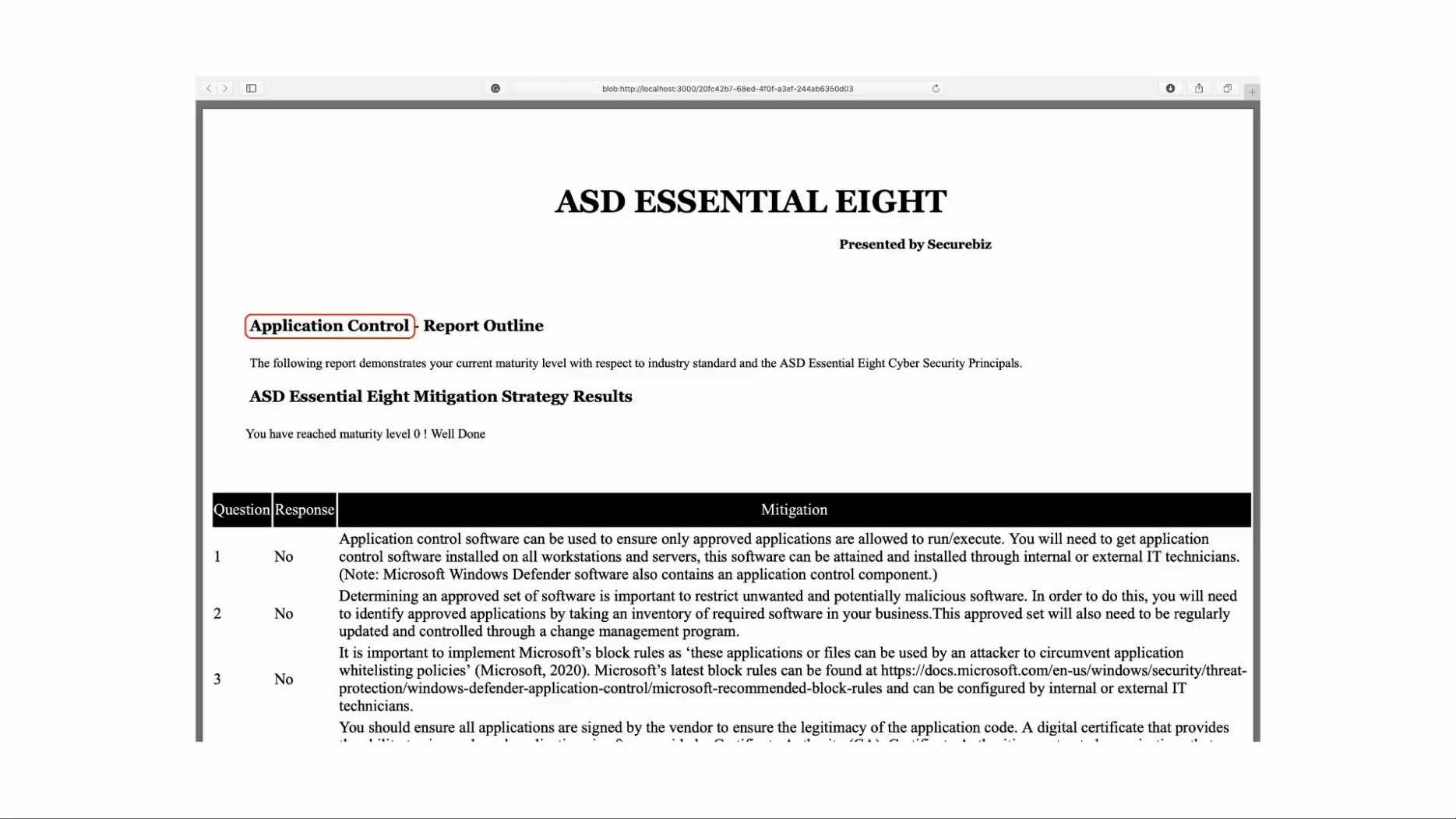


Figure 21: Application Control PDF report

The report outline contains a brief statement, followed by the maturity level achieved presented as a sentence similar to that shown on the front page at completion of the questionnaire, as discussed in section 3.1.

Following this introduction is a table containing the recommendations. This table has the headings of Question, Response and Mitigation; containing the question number, the text response as was selected by the respondent, followed by the paragraph of recommendations provided that explain why that response should be rectified.

### HTML Report

The HTML report will open in a new tab, with a file name that is a long, randomised string of alpha numeric characters. This file can then be saved from the browser as a PDF. The file itself consists of simple visuals aligned with the website itself. The text includes the ASD Essential Eight title, with ‘Presented by Securebiz’ emphasis, and the heading ‘Report Outline’. Following this brief intro, in bold, is the text “Mitigation assessed: [Mitigation Strategy]”, and following this, the maturity level is provided briefly as “You have reached maturity level X” with the emphasis in bold (Figure 22).

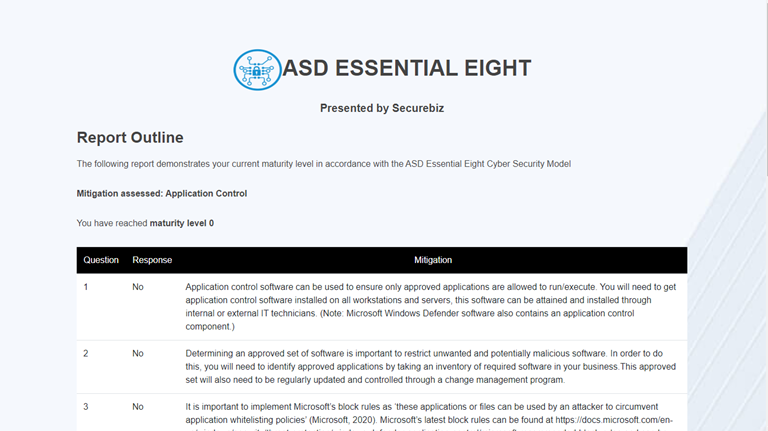


Figure 22: Application Control HTML report

As with the PDF, a table is provided containing the recommendations. This table has the headings of Question, Response and Mitigation; containing the question number, the text response as was selected by the respondent, followed by the paragraph of recommendations provided that explain why that response should be rectified.

## Providing the results to the client

As it stands, there is no formalized process to provide these reports to the client. In practice, this involves downloading these files to the consultant’s local environment, and providing them privately to the client within a encrypted .zip file.

# Admin Portal

The admin portal is currently a work-in-progress, as at time of writing, post MVP. The following briefly describes the current status of the Admin portal, however features are not yet functional.

The admin portal is the control panel through which an administrator may gain access to statistics about the data collected, and may alter the questions within the questionnaires. The user will be able to select the options of “Manage Mitigation Strategies” or “Statistics” from this screen, as discussed in section 3.4.

## 6.1 Manage Mitigation Strategies

The admin portal for management of the mitigation strategies is locked behind a login screen, which currently accepts the credentials “securebiz”/”securebiz” for administrator access (Figure 23). The admin login is currently functional, however the ‘Remember me’ and ‘forgot password?’ links are not.

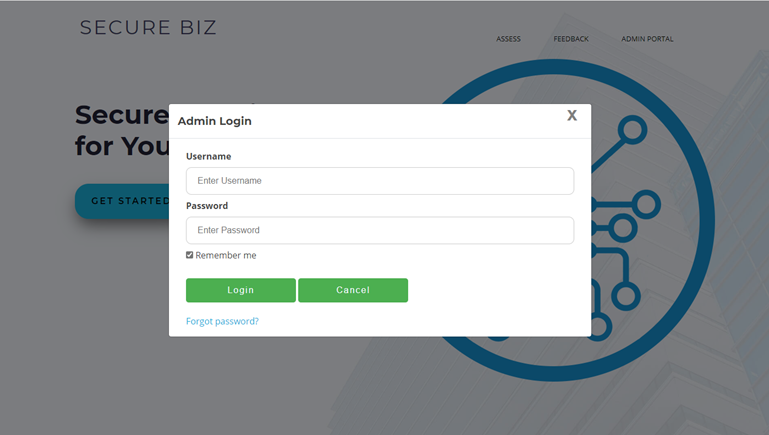


Figure 23: Admin Login

If the client is unable to provide valid credentials, they will be refused access, and an error will be shown to screen. If the username is incorrect, this error will be given as simple red text just below the ‘Admin Login’ pop-up heading with ‘Invalid username’ (Figure 24). If the password is incorrect the user will be shown the same with the text ‘Invalid password’ instead.

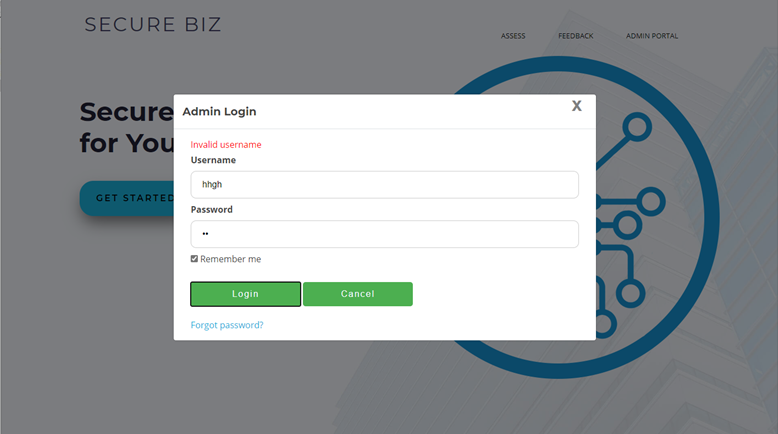


Figure 24: Admin Login with Invalid Username error

If the user is able to provide valid credentials, they are provided with three options from which to choose. These options do not currently connect, but in future will be used to gain access to change the questionnaires as according to the selection (Figure 25).

The options from which the administrator may choose are:

1. Add Mitigation
2. Edit Mitigation
3. List Mitigation

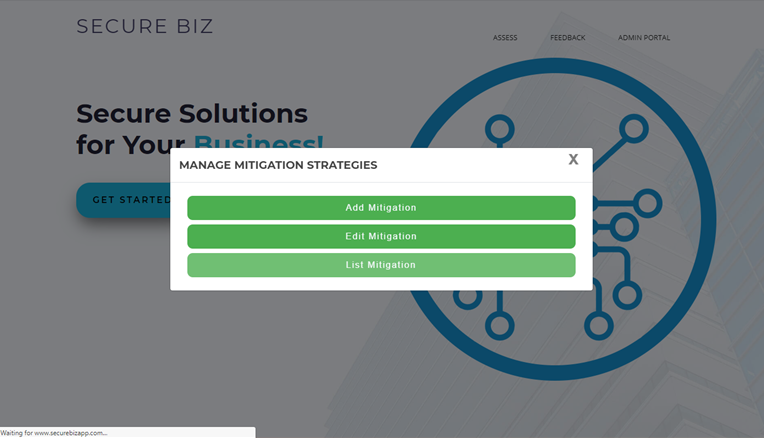


Figure 24: Admin Login with Invalid Username error

## 6.2 Statistics

The statistics option is not currently protected by a login screen, and the content when selected is a simple pop-up containing filler text.

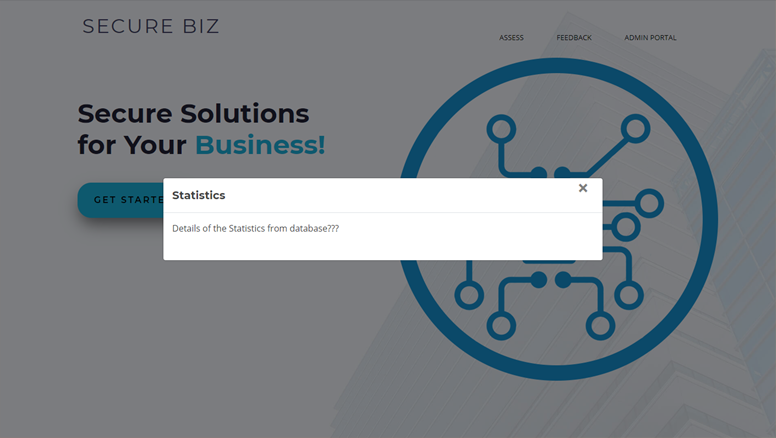


Figure 24: Admin Portal, Statistics selection

# System Capabilities and Constraints

The following section details specific components relating to the questionnaire structure and capabilities and restrictions which require consideration when making changes to the questions or refinement to the system.

Further detail about risks, considerations and decision-making processes for each of these items can be found in appendix item 8.5.

## Question Duplication

### 7.1.1 Summary

Within the extended questionnaire set of similar mitigation strategies, some questions will be relevant and included in both question sets.

### 7.1.2 Solution

Questions which are found to be effective duplicates of others will be aligned so that their wording, responses, and associated recommendations, where appropriate. These questions will be tagged in documentation as duplicates so that any required changes can be distributed fully and avoid misalignment.

These duplicate questions will appear during the completion of all relevant extended question set and are stored independently in the relevant collections under different keys. That is, if the user were to complete all questionnaires, they would be asked these questions multiple times with no indication they had responded previously.

### 7.1.3 Considerations

A technical solution for this constraint is pending implementation.

## Question Depth

### 7.2.1 Summary

Some questions may introduce the concept of depth, where a valuable question contains layers of complexity to reach the desired state, each of which should be determined. Such questions may not make sense to the user if a negative response is given to an earlier question.

i.e. The user is asked “Do you have a firewall?” and responds “No.” The following question is “Does your firewall have X setting enabled?” but the question should not be asked of a user who does not have a firewall.

### 7.2.2 Solution

Questions which follow a hierarchy as described will have an answer option included which is effectively a null response. The response will be worded as a statement which defines the lack of relevance for the user to respond to the question, and should be selected by the consultant based on the prior question, without requesting a response from the user.

i.e. Following the above example, the user is given the option to respond “I do not have a firewall.” to the second question.

Where a question response has been skipped by selecting this null response, the report produced will not include the recommendation associated with any other response to this question. The negative response to the preceding question should prompt sufficient detail in the recommendations in the report for the user to implement the appropriate changes.

### 7.1.3 Considerations

No Considerations.

## Additional Detail

### 7.3.1 Summary

Some question topics are necessary but rely upon complex or technical concepts accessible to all levels of knowledge which need to be catered for. Clients should be presented with the best opportunity to respond to a question accurately.

i.e. The user is asked “Have you disabled Object Linking and Embedding?” but the common user may not know what Object Linking and Embedding means, and therefore is unable to effectively respond.

### 7.3.2 Solution

Questions which contain complex or technical concepts will have an accompanying short paragraph which roughly explains the concepts touched upon in the response. This explanation will be brief and only contain the minimal amount of detail required to explain the concept in laymen’s terms, sufficiently for any system user to respond to, based on their use of the system.

In a question where this field has been filled, a question mark icon will appear on the question pop-up. Mouse-hover over this item will cause a text box to appear, containing the relevant explanation. When the mouse-hover is removed, the text box will disappear.

i.e. Following the above example, the user may hover over the (?) icon with their mouse and are presented with a short paragraph succinctly describing the concepts of Object Linking and Embedding in layman’s terms.

See section 3 for further detail.

### 7.1.3 Considerations

No Considerations.

## Response Tracking

### 7.4.1 Summary

The responses provided by the client indicate the state of the system at a specific point in time. The volume of work required to get their systems to the recommended maturity level is large, and the maturity levels are iterative to facilitate this. The system should contain methods to refer to previous states to smooth this iterative process.

### 7.1.2 Solution

Each time a client responds to a questionnaire in the system, a unique, randomised reference code is generated. This can be provided to the client for reference to their data, which is stored in the database with this reference code as a key.

### 7.1.3 Considerations

This solution may not be appropriate for storage of live user’s data, due to the security considerations. Appropriate assessment will be undertaken to ensure appropriate and secure handling of user’s data before the system is cleared for live testing. It is in the backlog for completion in a future sprint.

# Works Cited

Australian Cyber Security Centre, 2017. *Strategies to Mitigate Cyber Security Incidents.* [Online]   
Available at: https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents  
[Accessed 28 05 2020].

Australian Cyber Security Centre, 2019. *Implementing Multi-Factor Authentication.* [Online]   
Available at: https://www.cyber.gov.au/publications/implementing-multi-factor-authentication  
[Accessed 28 05 2020].

Australian Cyber Security Centre, 2019. *Restricting Administrative Privileges.* [Online]   
Available at: https://www.cyber.gov.au/publications/restricting-administrative-privileges  
[Accessed 28 05 2020].

Australian Cyber Security Centre, 2019. *You need to patch to protect your business online.* [Online]   
Available at: https://www.cyber.gov.au/news/patch-to-protect-your-business  
[Accessed 28 05 2020].

Australian Cyber Security Centre, 2020. *Assessing Security Vulnerabilities and Applying Patches.* [Online]   
Available at: https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches  
[Accessed 28 05 2020].

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

Australian Cyber Security Centre, 2020. *Guidelines for System Hardening.* [Online]   
Available at: https://www.cyber.gov.au/ism/guidelines-for-system-hardening   
[Accessed 28 05 2020].

Australian Cyber Security Centre, 2020. *Implementing Application Control.* [Online]   
Available at: https://www.cyber.gov.au/publications/implementing-application-control  
[Accessed 28 05 2020].

Field, A., 2003. *Discovering Statistics.* [Online]   
Available at: http://www.discoveringstatistics.com/docs/designing\_questionnaires.pdf  
[Accessed 27 05 2020].

Fisher, S., 2020. *11 Tips for building effective surveys.* [Online]   
Available at: https://www.qualtrics.com/blog/10-tips-for-building-effective-surveys/  
[Accessed 27 05 2020].

Harrison, C., 2007. *TIP SHEET ON QUESTION WORDING.* [Online]   
Available at: https://psr.iq.harvard.edu/files/psr/files/PSRQuestionnaireTipSheet\_0.pdf  
[Accessed 27 05 2020].

Lloyd, S., 2018. *The 10 commandments for writing good surveys and questions.* [Online]   
Available at: https://www.qualtrics.com/blog/good-survey-questions/  
[Accessed 27 05 2020].

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

National Institute of Standards and Technology, 2020. *Cybersecurity.* [Online]   
Available at: https://www.nist.gov/topics/cybersecurity  
[Accessed 28 05 2020].

Survey Monkey, 2020. *Survey Guidelines.* [Online]   
Available at: https://www.surveymonkey.com/mp/survey-guidelines/  
[Accessed 27 05 2020].

Survey Monkey, 2020. *Writing good survey questions.* [Online]   
Available at: https://www.surveymonkey.com/mp/writing-survey-questions/  
[Accessed 27 05 2020].

Tech Republic, 2018. *5 common browser security threats, and how to handle them.* [Online]   
Available at: https://www.techrepublic.com/article/5-common-browser-security-threats-and-how-to-handle-them/  
[Accessed 28 05 2020].

techopedia, 2012. *Object Linking and Embedding (OLE).* [Online]   
Available at: https://www.techopedia.com/definition/4995/object-linking-and-embedding-ole  
[Accessed 28 05 2020].

# 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)

## Change Management

This document can be found locally [here](https://teams.microsoft.com/l/file/A4C651B5-4EAB-464A-9B1C-C1F007B7C13A?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%2FHandover%20Artefacts%2FQuestionnaires%20and%20Mitigation%20Strategies%2FQuestion%20Change%20Log%20MVP.xlsx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9).

## System Capabilities and Constraints solution considerations

### 8.5.1 Question Duplication

#### 8.5.1.1 Summary

Within the extended questionnaire set of similar mitigation strategies, some questions will be relevant and included in both question sets.

#### 8.5.1.2 Risks

* Encountering the same question multiple times in several different contexts may result in frustration and loss of quality of user experience. – “I have already answered this.”
* The creation of multiple versions of the same question results in duplication of work for strategists to produce and refine said questions, where efforts could be used elsewhere.
* The encoding of multiple versions of the same questions results in duplication of work for programmers, to include questions within the question sets
* Redundancy of information stored within the database causes unnecessary storage burdens upon the system.
* Very similar yet not identical questions may introduce confusion or discrepancies within the system. This includes updating one question but not another, which may result in discrepancies in responses from the user.
* Improvement of a question or associate mitigation strategy may be impeded by multiple untracked change locations, at risk of introducing confusion or discrepancies within the system and additional work to identify all duplicates of the given question.

#### 8.5.1.3 Considerations

* The user may respond to a question set and provide a response to the question at a point in time and receive and act upon the feedback for that question set, before completing another set. This may result in a different response at that later time. If the question it not asked again, feedback will not be appropriate for the later state of the product.
* The mitigation strategies do not have a distinct and defined order of completion, so prioritization of a question in one questionnaire does not permit the assumption that it has been considered, later.
* The questions may not be perfect duplicates; possibly worded slightly differently or the considerations in the response focuses more closely with the risks associated with the mitigation strategy for which it appeared within the questionnaire.

#### 8.5.1.4 Possible solutions

##### Non-Technical

* Question is produced for each questionnaire, standalone and not linked, and are asked each time the relevant questionnaire is completed. Duplication of the question occurs, but the accurate response is recorded at the time of completion.

##### Technical

* Enabling response retrieval to inform the consultant of a prior response to a linked or identical question may allow the consultant to determine whether the question should be asked again and the response altered based on their knowledge of the client, rather than a prompting by the system.
* A selection accessible above, or in the entry point to a questionnaire which asks whether the user has implemented any changes to their security since last check in, may inform the system to ask duplicated questions again to get an updated response.
* An “I’ve already responded to this” escape option for a specific question in the questionnaire may allow the consultant, or client upon prompt, to move past a duplicated question.

#### 8.5.1.5 Relevant Standards

No relevant standards currently identified.

### 8.5.2 Question Depth

#### 8.5.2.1 Summary

Some questions may introduce the concept of depth, where a valuable question contains many layers to reach the desired state, each of which should be determined. Such questions may not make sense to the user if a negative response is given to an earlier question.

#### 8.5.2.2 Risks

* Upon answering negatively to an upper level question, if the client is asked a question of greater depth it may result in confusion, repetition, frustration and loss of quality of user experience. – “These questions are irrelevant as the question is obvious, given my earlier response.”

#### 8.5.2.3 Considerations

No considerations.

#### 8.5.2.4 Possible solutions

No relevant standards currently identified.

##### Non-Technical

* The Consultant recalls the response given earlier and skips the lower level questions by selecting the negative response to all relevant questions, resuming the questionnaire

##### Technical

* Enabling response retrieval to prefill a response to a question based on an earlier question may allow the consultant to respond to the question without requesting the response from the user with discretion towards the specific circumstances of the client.
* A consultant instruction label could be included to directly inform the consultant of questions with later dependencies and dependent questions, so that they may manually propagate the response to these questions with greater accuracy.
* Inclusion of question masking to obscure or remove lower level structures from the questionnaire upon a negative response.

#### 8.5.2.5 Relevant Standards

No relevant standards currently identified.

### 8.5.3 Additional Detail

#### 8.5.3.1 Summary

Some question topics are necessary but not necessarily accessible to all levels of knowledge which need to be catered for. Clients should be presented with the best opportunity to respond to a question accurately.

#### 8.5.3.2 Risks

* Questions which relate to complex concepts that are not able to retain value when distilled to natural language, if so, may not accurately capture the current state of the system.
* Where jargon is used, the client may not be able to respond, and may feel frustrated or embarrassed by lack of knowledge, reducing the quality of their user experience.
* Where jargon is necessary and the questions cannot be reduced to natural language, the client may be unable to respond accurately, reducing the quality of information collected.
* If the consultant is required to explain the concepts to the client in order to assist them in responding, the consultant may provide out of date, incorrect or misleading information, deliberately or by mistake, preventing the client from responding accurately.

#### 8.5.3.3 Considerations

* The user may or may not require additional detail in order to accurately respond to the question.
* Not recognising or responding to jargon in a question or a specific phrasing of a question does not necessarily mean that the client should respond to the question negatively.
* Similarly, the client may mistake a concisely described question, which uses low-level language as a mitigation strategy they have in place, when in truth, it is not, or else is not to the extent intended by the question.
* Large chunks of text or excessively worded or detailed questions introduce a difficulty for the client to follow, and therefore respond accurately.

#### 8.5.3.4 Possible solutions

##### Non-Technical

* The consultant understands the detail behind every question contained within the survey, and is able to comfortably and effectively explain the concepts to the client to equip the client with the necessary detail to respond.

##### Technical

* A “more information” section appears on the question for each question where it may be necessary, and the consultant is able to read this out to provide scripted relevant information to the client upon request.
* A “more information” expandable section appears on the question for each question where it may be necessary, and the consultant can click on this area to make the text visible in page, therefore reducing page clutter if it is not required, or once it is no longer required.

#### 8.5.3.5 Relevant Standards

No relevant standards currently identified.

### 8.5.4 Response Tracking

#### 8.5.4.1 Summary

The responses provided by the client indicate the state of the system at a specific point in time. The volume of work required to get their systems to the recommended maturity level is large, and the maturity levels are iterative to facilitate this. The system should contain methods to refer to previous states to smooth this iterative process.

#### 8.5.4.2 Risks

* User experience may be inhibited by repeating previous steps at each step of the iteration, and improvements to security profile cannot be tracked using the app.
* Storage of user data requires implementing security methods on the product itself, especially for the use-case described, as for a cybercriminal, this data represents a clear cut list of the security vulnerabilities of a client.

#### 8.5.4.3 Considerations

* Users may wish to refer to the previous state answers and compare that to current state within the system to log updates.

#### 8.5.4.4 Possible solutions

* With the PDF output provided, the user may be provided with a string of code which can be provided back into the system to generate their response at that time, again. This would allow storage of the sensitive data only in the hands of the client, as the information would not need to be stored in the product itself. Functionality would need to be written to encode the answers and read the encoded answers back into the database. Alterations of the question sets would need to be considered to preserve this snapshot of state. This would be a round-about way to do this, but removes security responsibility from the product in the early instances while still making it possible to refer to prior state within the system.

*Example: User has responded “Yes” to MFAMA1, MFAMA2 and “No” to MFAMA3. They have not responded to MFAE1-10.   
They may be provided with the code: 1M01.1|1M02.1|1M03.2|1E01.0|1E02.0|…|1E10.0  
read as |<Mitigation Strat ID Number><QuestionSet(E/M)><QuestionID>.<ResponseCode>| which can then be read back into the system by splitting into questions on | and then identifying the question itself, and inserting the response code.*

* Implementing sufficient security measures around data storage, it would be most valuable to make it possible to save and retain the client’s response data, along with a timestamp for the date given, and retrieve this for consideration later.

#### 8.5.4.5 Relevant Standards

No relevant standards currently identified.