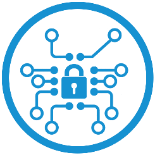
T1

2021

Cyber Security Capability and Maturity Consultancy Services Project

 Starter Kit

ASD ESSENTIAL EIGHT CYBER MIGRATION TOOLKIT

ASD ESSENTIAL EIGHT SIT782 CLASS OF T3 2020

Table of Contents

[Change Management 2](#_Toc62065551)

[Introduction 3](#_Toc62065552)

[1. Management 4](#_Toc62065553)

[1.1 On Track 4](#_Toc62065554)

[1.2 Meetings and Contact frequency 4](#_Toc62065555)

[1.3 Work Tasks 4](#_Toc62065556)

[1.4 Representation 5](#_Toc62065557)

[1.5 Record of work 5](#_Toc62065558)

[2. Sections 6](#_Toc62065559)

[2.1 Management and Documentation 6](#_Toc62065560)

[2.2 Application Security 8](#_Toc62065561)

[2.3 Design and Planning 9](#_Toc62065562)

[2.4 Development and Build – Front End 10](#_Toc62065563)

[2.5 Development and Build – Back End 11](#_Toc62065564)

[2.6 Testing and Deployment 12](#_Toc62065565)

[3. Documentation 13](#_Toc62065566)

[3.1 Overarching Documentation 13](#_Toc62065567)

[3.2. Questionnaire and mitigation strategy 13](#_Toc62065568)

[3.3 Front-end and back-end documentation 13](#_Toc62065569)

[3.4 Report documentation 14](#_Toc62065570)

[3.5 Security documentation 14](#_Toc62065571)

# Change Management

|  |  |  |
| --- | --- | --- |
| **Date** | **Contributor** | **Summary of Contribution** |
| 20/01/2021 | Micheal Cumming | Moved into git and removed version from filename. |
| 24/01/2021 | Micheal Cumming | Amendments from Andrew Hall & Update filenames |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Introduction

The ASD Essential Eight Project centres around the ASD Essential Eight; eight cyber security areas of consideration for which the Australian Signals Directorate has supplied specific baseline standards for cyber security. The eight areas have been identified as having the greatest influence over the security of a business’ cyber infrastructure.

This project makes use of the ASD Essential Eight to create a product that can be used by a cyber security consultant to assess the maturity of a client’s security infrastructure. This assessment is completed by way of a questionnaire, and algorithms that take the client’s responses and converts them to a report with a maturity level received and a set of recommendations for how to improve.

Formally, the project overview is as follows:

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

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

From the Overarching documentation item 2. Project Overview

In the following sections you will find:

1. Information on the more general management aspect of the project and the requirements of the team
2. Information on the existing team, the roles available and division of work, and where you may find yourself contributing
3. Finally, some choice excerpts from the overarching documentation which may direct you to where you can find more specific information on any particular project topic

Please remember that the seniors are here to help you and are very eager to assist in any way we can to get you involved and integrated into the squad.

Here is the make-up of the team and welcome to the new Junior members.

|  |  |  |
| --- | --- | --- |
| **Start Date** | **Level** | **Team Member Name** |
| T3 2021 | Senior | Raymond **Corrigan** |
| T3 2021 | Senior | Micheal **Cumming** |
| T3 2021 | Senior | Andrew **Hall** |
| T3 2021 | Senior | Ben **Landers** |
| T3 2021 | Senior | Hugo **Ng** |
|  | Junior |  |
|  | Junior |  |
|  | Junior |  |
|  | Junior |  |
|  |  |  |

# Management

As a student undertaking the SIT764/SIT782 unit, you will be responsible for:

* Completing your own OnTrack tasks and contributing towards the squad OnTrack tasks
* Attending all required meetings and checking MS teams regularly
* Taking initiative in seeking work tasks
* Seeking opportunities to represent yourself and your capabilities in the best possible light
* Ensuring you keep appropriate records of work completed

You will have help from your fellow students to meet these expectations, and in addition, you will have a senior in your section who will act as a mentor.

## 1.1 On Track

OnTrack is the assessment application used by the unit to provide assessment task sheets and resources, and to allow students to communicate their progress individually with the Unit Chair. Some Junior assessment items differ from the Seniors and may differ from the semester when the seniors completed their junior unit. The seniors are happy to provide advice and support for completion of tasks, but you may need to reach out to seek this support, as we will not be also completing these tasks.

Demo tasks and individual retrospectives are due at the end of each iteration, and both seniors and juniors complete these tasks the same, except for Iteration 0. The Demos are a group assessment item and are usually directed by the Project Management team with directed involvement from all other team members.

***Note:*** *OnTrack tasks are at times revised with only a few days’ notice for the changes. Ensure that you will have adequate opportunity to respond and make alterations in the week prior to the task submission if you intend to complete your tasks early.*

## 1.2 Meetings and Contact frequency

We have a regular meeting at 8pm Wednesdays (Melbourne time) with the squad supervisor, and additionally one meeting time during the week at a time suitable to all parties. Squad meetings begin with a quick stand-up; this is a brief statement of *done, next and blockers*, and is passed from person to person with each person nominating the next when they finish providing their update. Further agendas are provided on the meeting thread in the lead up to the meeting.

Aside from the set meetings, there are no explicit times that team members are expected to be active on teams. However, all squad members should check teams regularly, (every 2 days or less is highly recommended), to stay on top of any changes and ensure they are not blocking other member’s work.

## 1.3 Work Tasks

Work tasks are managed via Trello and may be self-allocated or delegated depending on the dynamic and work demands of your section. The Trello board can be accessed from the top tabs in the Teams channel. Please join as a guest and you will then be added as a permanent member. Please use the following links to get yourself for the two (2) Trello boards.

**Roadmap Trello Board:** [Invite](https://trello.com/invite/b/OWFJrike/105d195e364f947b6cec7426a8209819/asd-essential-eight-cyber-mitigation-toolkit-roadmap)

**Main Project Trello Board:** [Invite](https://trello.com/invite/b/kcFFf5ya/d55e6518fca29eaae98f01b09e88beb6/asd-essential-eight-cyber-mitigation-toolkit-trello)

The board tasks are split into sections represented as columns. Task progression is marked as labels applied to the cards. The cards themselves should be kept up to date, the forwards progression of work, users and due dates can be assigned to these cards.

## 1.4 Representation

The assessment process in this unit is self-managed, and you will need to ensure that you seek a range of work and roles that suit your capabilities in addition to the assessment criteria.

It is strongly suggested you take the opportunity before commencement of the new iteration, to look through the assessment criteria with a heavily critical eye and determine exactly which level you’re intending to claim for each criterion, and how you can provide evidence to support your claim. Your senior counterparts have completed a number of these assessments before and are happy to provide advice and guidance if needed.

## 1.5 Record of work

You are required to keep a record of the work you have completed in this unit from the first week. As a member of the squad, you will be given access to the squad workbook and this is the formal location in which you will need to record your hours. The workbook (Workbook T1 2021) can be found within the 'T1 2021 Files' folder, located in the Files tab along the top of the channel and you will need to maintain this and ensure it is up-to-date at the end of each iteration in preparation for the squad demo.

Keep a record of your personal worklog entries in a secondary location in case there are any errors in the worklog, and data is lost. Time is only recorded in 10-minute increments so take care with your rounding and ensure that you break time blocks down as much as is reasonable into the individual tasks completed. The longest a single task can go for is 240 minutes, but it is unlikely you will be producing 240-minute blocks (4 hours) of the single piece of work, straight. You may be required to justify the hours you claim, so ensure that your descriptions are concise but meaningful and representative of the time committed.

Worklog can be found in the MS SharePoint / MS Teams folder for the current Trimester and is called “WorkLog Tx yyyy.xlsx” for example Worklog T3 2020.

Graphical user interface

Description automatically generated with medium confidence

*Figure One – Team Structure for T3 2020*

# 2. Sections

Please refer to Figure One for the current Team structure.

Each section represents a body of work and area of responsibility within the squad. Each section may have more than one member. While every member has a defined role, members are more than welcome to work across disciplines and assist others in different areas.

There is strong cross-over between each of these sections with others and not all work will fall neatly into any bucket. The section structure does not dictate who will complete what work, but rather gives accountability for that area to a single person; for both the work that needs to be done and direction over who will complete it.

## 2.1 Management and Documentation

The Management and Documentation section deals with the stakeholder and project management aspects of the project, including iteration demos, scrum calls, updates, and retrospectives. The documentation aspect also includes the continuation and refinement of the existing project documentation, and alignment between the sections. The role consists of:

* Planning and running the squad meetings
* Providing whole-of-squad updates to the project supervisor and staying on top of squad happenings.
* Taking meeting minutes via meeting recordings and providing these to the team as a record.
* Being the direct contact for any issues regarding the squad.

There are the following cross-over responsibilities:

* With Design: Ensuring the work prioritization meets the required timelines for project deliverables.
* With Application Security: Stewardship of document creation processes for the creation of the “Security” Documentation
* With Build: Upkeep of the front-end and back-end technical documentation.

A Project Management and documentation team member would benefit from having the following skills or interests:

* Agile project development
* People management
* Strong communication and written English
* Attention to detail
* Intention to read the existing documentation

A Project Management and Documentation team member should upskill in the following:

* ASD Essential Eight and Maturity Model
* Scrum and Agile ceremonies
* Agile documentation practices
* Stakeholder management
* Rudimentary understanding of: Cyber Security, web application languages (HTML, Javascript, CSS), databases (esp MongoDB)
* Documentation: Flow diagrams, communication of technical concepts

## 2.2 Application Security

The Application Security section deals with the internal security matters of the SecureBiz application, from login to completion and provision of the results. As the data we collect deals with the strengths and weaknesses in a business’ cyber infrastructure, it would be dangerous in the wrong hands and therefore is considered highly sensitive. The role consists of:

* Assessing the current build against cyber security best practice
* Articulating the severity of noted risks and weighing the security risk against usability

There are the following cross-over responsibilities:

* With Design and Planning: Generating designs or build requests for inclusion in the backlog and prioritisation.
* With Build: Implementing build items.
* With Testing: Penn testing, bug follow-up for Application Security items
* With Management: Production and refinement of the “Security” documentation

An Application Security team member would benefit from having the following skills or interests:

* Application Security
* Database Security
* OSI model (Networking)
* Scripting (PowerShell/Bash)
* Cryptography (SSL)

An Application Security team member should upskill in the following:

* ASD Essential Eight and Maturity Model
* MongoDB
* Visual Studio
* Fundamentals of: SQL Injection, XSS
* Security tools: Nmap, Acunetix, Burb suite, Owasp, Wireshark, Nikto (all tools can be found at offensive Security (Parrot Security OS))
* Rudimentary understanding of: HTML/PUG (JADE), Bootstrap, Express .js and Node. Js, JavaScript, CSS, JSON,

This role would be beneficial for a student undertaking a degree with a cyber security focus.

## 2.3 Design and Planning

The Design and Planning section are responsible for determining the direction of the application, akin to an internal product owner. They produce designs for build items based on the project deliverables and prioritise them in the backlog to be picked up by the build team. The role consists of:

* Assessing the current state of the application and the work required to meet the minimum viable product.
* Articulating the components of work into build requests, including the parameters and acceptance criteria of the items.

There are the following cross-over responsibilities:

* With Application Security: Stewardship of the design process for Application Security items
* With Build: Communication of requirements and acceptance criteria for build requests.
* With Testing: Bug follow-up
* With Management: Accountability for project direction

A design team member should have the following skills or interests:

* Agile project development
* Strong communication and written English
* Attention to detail

A design team member should upskill in the following:

* ASD Essential Eight and Maturity Model
* Scrum and Agile ceremonies
* Agile documentation practices
* Stakeholder management
* User story and Acceptance Criteria
* Solid understanding of: Cyber Security, web application languages (HTML, Javascript, CSS), databases (esp. MongoDB)

## 2.4 Development and Build – Front End

The build teams are responsible for creating the code and implementing it inside the development environment of the SecureBiz application. The Front-End build team specifically works with the user interface. The role consists of:

* Building UI features in accordance with acceptance criteria
* Managing the quality of the code
* Completing rudimentary testing of code on commit

There are the following cross-over responsibilities:

* Application Security and Design: Discussing, prioritising, and completing build requests from the backlog
* Management: Consultation for the ongoing management of the technical documentation
* Testing: Deployment of functional code for UAT, bug fixes

A Front-End Build team member should have the following skills or interests:

* User experience and code design
* Web application building
* Coding (HTML, JavaScript, CSS)

A Front-End Build team member should upskill in the following:

* ASD Essential Eight and Maturity Model
* MongoDB
* HTML/PUG (JADE), Bootstrap, Express .js and Node. Js, JavaScript, CSS, JSON, React and OpenAPI
* Visual Studio
* Coding/Programming best practices

This role would be beneficial for a student undertaking a degree with an Information Technology focus.

## 2.5 Development and Build – Back End

The build teams are responsible for creating the code and implementing it inside the development environment of the SecureBiz application. The Back-End build team specifically works with management and interaction with the database, and calls from the UI to the various application components. The role consists of:

* Building the back-end code to support features and services in accordance with acceptance criteria
* Managing the quality of the code
* Completing rudimentary testing of code on commit
* Managing Database
* Integration of code completed last semester

There are the following cross-over responsibilities:

* Application Security and Design: Discussing, prioritising, and completing build requests from the backlog
* Management: Consultation for the ongoing management of the technical documentation
* Testing: Deployment of functional code for UAT, bug fixes.

A Back-End Build team member should have the following skills or interests:

* Code design / code review
* Database management
* Knowledge of code integration
* Rudimentary front-end application building knowledge

A Back-End Build team member should upskill in the following:

* ASD Essential Eight and Maturity Model
* MongoDB
* Bootstrap, Express .js and Node. Js, JSON, JavaScript, Mongoose and OpenAPI.

This role would be beneficial for a student undertaking a degree with an Information Technology focus.

## 2.6 Testing and Deployment

The testing and deployment team is responsible for quality assurance checks on the code released, and management of the deployment to a secondary testing environment, UAT, for UAT. The role consists of:

* Preparing test plans to broadly check the health of the system
* Preparing test plans for specific new functionality to pointedly check aspects of that functionality
* Managing, storing, and reviewing test execution evidence.
* Writing testing reports
* Declaration and communication of bugs

There are the following cross-over responsibilities:

* Application Security: Penn testing
* Design and Planning: Communication and prioritisation of bugs for bug fixes
* Build: Deployment of code for testing, identification, or root cause of bugs
* Management: Answerable for Quality Assurance

A testing team member should have the following skills or interests:

* Quality assurance
* Attention to detail
* Consideration of user experience
* Knowledge and technical skills
* Experience in UAT

A testing team member should upskill in the following:

* ASD Essential Eight and Maturity Model
* MongoDB
* Bitbucket
* PowerShell
* Test Driven Development
* Agile Testing

# 3. Documentation

This section contains choice elements adapted from the Overarching Documentation, item 3. Purpose of the overarching documentation.

Table 2 provides a list of the documents produced as part of development in T12020 and will be continuously improved and updated as the project progresses. Team members may consult these documents to obtain in depth knowledge about project components, however it is not required to read these as part of the introduction to team.

We do recommend that team members new to the project look over the overarching documentation, as this touches upon most of the key elements of the project and is supremely useful for understanding the project scope and deliverables.

*Table 2 - Documentation*

|  |  |
| --- | --- |
| **Document File Name** | **Purpose** |
| ASDE8 Overarching Document | Top level documentation |
| ASDE8 Requirements Document | Requirements Documentation |
| ASDE8 Questionnaire and Mitigation Strategy | Non-technical Product Definition |
| ASDE8 Frontend and Backend | Architectural documentation for the front-end and back-end |
| ASDE8 Admin Portal | Admin Portal Design Document |
| ASDE8 Reporting | Reporting and PDF Specification |
| ASDE8 New Starter Checklist | Checklist for onboarding new starters |

## 

## 3.1 Overarching Documentation

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

This document also collates the other technical documentation created; a summary of the project’s documentation can be seen in the sections following. The document can be found [here](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/T3%202020%20Files/Project%20Management/Documentation/Overaching%20documentation.docx?d=wec018778fd554877a2e346489cf91fab&csf=1&web=1&e=fGqu6l).

## 3.2. Questionnaire and mitigation strategy

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

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

## 3.3 Front-end and back-end documentation

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

## 3.4 Report documentation

The report documentation contains the technical aspects of the report collation and coding. This report is contained within the front-end and back-end documentation [here](https://deakin365.sharepoint.com/:w:/r/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/T3%202020%20Files/Project%20Management/Documentation/report%20t3.docx?d=w791e0d1a936f4cfa91b6d4b1f645c62a&csf=1&web=1&e=sH8lQW).

## 3.5 Security documentation

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

\_\_\_