



Essential Eight Assessment Report [ENTITY NAME]

Status: [DRAFT/FINAL]

Instruction: This template provides the content requirements of essential eight assessment reports. Assessors can use their own report templates for branding purposes however all sections within this template must be included. Delete this and all other instructions from your final version of this document as well as Australian Signals Directorate (ASD) branding. For guidance on how to conduct an assessment, refer to the *Essential Eight Assessment Process Guide*.

Document details

Assessment

Assessment Details	
Essential Eight version	<Month YYYY>
System security classification	Choose an item.
Report template version	V1.1

Prepared by

Assessor Organisation Name	
<div></div>	Address
	Assessor name
	Assessor qualifications
	Contact email

Prepared for

Entity Name	
<div></div>	Address
	Contact name
	Contact email

Revision history

Version	Date	Description	Author
---------	------	-------------	--------

||
||
||

Table of contents

Executive summary	1
Introduction	2
Background	2
Scope	2
Approach	2
Limitations	2
Detailed findings	3
Application control	3
Patch applications	3
Configure Microsoft Office macro settings	3
User application hardening	4
Restrict administrative privileges	5
Patch operating systems	6
Multi-factor authentication	6
Regular backups	7
Summary of recommendations	10
Appendix A – Assessment evidence	11

Executive summary

Instruction: Provide a one-to-two-page overview of the assessment including:

- brief background on the entity and system being assessed
- assessment scope, approach and limitations
- summary of Essential Eight maturity
- summary of key security risks and positive findings identified during the assessment
- summary of key recommendations to remediate security risks and/or achieve the target maturity level.

DRAFT

Introduction

Background

Instruction: As appropriate, provide a one-to-two-page introduction to the Essential Eight, the entity and their operating environment, their cyber security strategy, and any recent cyber security uplift activities or prior Essential Eight assessments.

Scope

Instruction: Detail the system under assessment (including the system boundary and any exclusions), the version of the Essential Eight being used and the target maturity level.

Approach

Instruction: Detail the approach used to assess the system including:

- qualitative and quantitative techniques used for testing security controls
- sampling technique and rationale for sample sizes
- specific tools used during the assessment, such as scripts and vulnerability scanning tools.

Limitations

Instruction: Detail any assessment limitations, for example, availability of information, resources or technical testing constraints.

Detailed findings

Application control

Findings

Instruction: Provide comments on the assessment of the mitigation strategy's implementation including:

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)
- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD's implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

[illegible]

Recommendations

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

Patch applications

Findings

Instruction: Provide comments on the assessment of the mitigation strategy's implementation including:

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)

- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD's implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

[illegible]

Recommendations

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

Configure Microsoft Office macro settings

Findings

Instruction: Provide comments on the assessment of the mitigation strategy's implementation including:

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)
- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD's implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

Requirement	Implementation Status	Test Type	Assessment Justification

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

User application hardening

Findings

Instruction: Provide comments on the assessment of the mitigation strategy's implementation including:

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)
- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD's implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

[illegible]

Recommendations

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

Restrict administrative privileges

Findings

Instruction: Provide comments on the assessment of the mitigation strategy's implementation including:

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)
- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD's implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

[illegible]

Recommendations

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

Patch operating systems

Findings

Instruction: Provide comments on the assessment of the mitigation strategy's implementation including:

<Classification//Sensitivity>

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)
- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD's implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

[illegible]

Recommendations

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

Multi-factor authentication

Findings

Instruction: Provide comments on the assessment of the mitigation strategy's implementation including:

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)
- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD's implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

Requirement	Implementation Status	Test Type	Assessment Justification
-------------	-----------------------	-----------	--------------------------

Recommendations

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

Regular backups

Findings

Instruction: Provide comments on the assessment of the mitigation strategy’s implementation including:

- whether requirements at the target maturity level were achieved
- how the requirements at the target maturity level were tested
- how the requirements at the target maturity level were implemented (or not)
- justification for the assessment outcome.

Note, the implementation status of each requirement should reflect ASD’s implementation definitions of Effective, Not Effective, Alternate Control, Not Applicable, Not Implemented or Not Assessed.

Requirement	Implementation Status	Test Type	Assessment Justification

Recommendations

Instruction: Detail any recommendations to mitigate deficiencies in the implementation of requirements in order to achieve the desired maturity level for the mitigation strategy.

DRAFT

Summary of recommendations

Instruction: List all the recommendations for reaching the target maturity level of the assessment.

DRAFT

Appendix A – Assessment evidence

Instruction: As required, provide evidence to support assessment findings and conclusions made, for example, screenshots of configuration and scanning results.

DRAFT