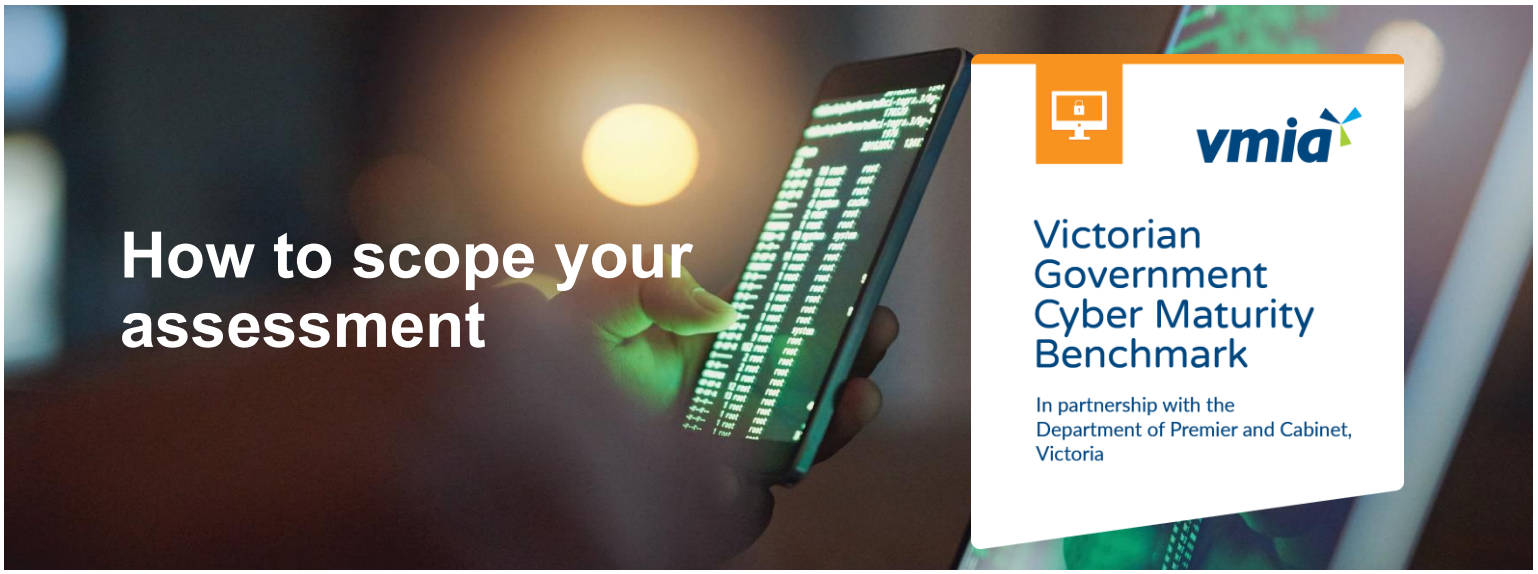

This guide's designed to help you make a risk-based assessment of your corporate environment against the Essential Eight control strategies in the Cyber Maturity Benchmark.

After completing the assessment, you'll know how to implement the security controls and strategies in the Essential Eight model to prevent, limit, and recover from cyber incidents.

The assessment's based on the concept of **maturity**. This means there's a range of good practices from a basic level to a more advanced approach. The concept recognises that organisations can choose a level of maturity in line with their risk, ambition, and available budget.

Approach

You'll need to use different methods to gather the information needed to assess your maturity. We suggest you:

- Scope your Essential Eight assessment
- Identify required resources – e.g. specialists, audit resources, tools
- Review relevant documents – e.g. security policies
- Assess selected system-based controls
- Interview key stakeholders – e.g. ICT managers, cyber security professionals, suppliers including any Managed Service Provider (MSP) for ICT services

Scope

The Essential Eight maturity model's valuable for:

- servers
- jump hosts
- workstations

To help identify the parts of your IT systems you should include in your assessment, refer to Australian Cyber Security Centre (ACSC) publications. E.g. "How to prepare for, protect against and respond to cyber security incidents" section of the ACSC 2020-2021 Annual Cyber Threat Report

Can I include cloud environments in scope?

The Essential Eight was designed for organisational corporate environments and may not suitably protect cloud environments. However, organisations should make risk-based decisions when identifying if cloud-based environments and services should be included in the assessment.

Limits on scope

Organisations may choose not to evaluate:

- operational technology (OT) environments (however they can consider including it as a separate sub-assessment)
- cyber security controls outside of the management of the organisation (unless supported by their MSP)
- broader organisation cyber security management arrangements

VMIA is the Victorian Government's insurer and risk adviser
Level 10 South, 161 Collins Street Melbourne VIC 3000
P (03) 9270 6900 contact@vmia.vic.gov.au ABN 39 682 497 841
vmia.vic.gov.au

Victorian Managed Insurance Authority (VMIA) acknowledges the Traditional Custodians of the land on which we do business and we pay our respects to their Elders, past, present and emerging. We acknowledge the important contribution that Aboriginal and Torres Strait Islander Peoples make in creating a thriving Victoria.

D22/43085 V.3 2022-04-19

Assessment methodology

Organisations should make a risk-based decision on the assessment or audit method they use, based on the level of assurance their organisation wants to achieve.

You can access tools to help you assess your maturity through the Department of Premier and Cabinet's (DPC) Cyber Safety Unit.

Further guidance

How should I work with my managed service provider to complete the assessment?

For guidance on working with managed service providers to complete your assessment, refer to the Improving Cyber Maturity with the Essential Eight guide. Organisations should seek appropriate assurance based on the risk from their MSP on the application of the Essential Eight control strategies.

Should I apply Essential Eight mitigation strategies to Linux and Unix systems?

Yes, apply Essential Eight control strategies that are applicable to Linux and Unix systems. The ACSC provides guidance for applying the Essential Eight in Linux Environments.

Is the Essential Eight applicable to Operational Technology (OT) / Industrial and Automated Control Systems (IACS)?

Four of the Essential Eight mitigation strategies are considered applicable to OT/IACS:

- application control
- patch applications
- restrict administrative privileges
- patch operating systems.

For guidance on protecting control systems, the ACSC refers to the Seven Strategies to Defend ICS from the U.S. Department of Homeland Security.

Should public facing systems/services be considered as part of the assessment?

Yes. Public facing systems and services can be included due to the associated risk of cyber-attack.

Should I list mitigating controls in the comments?

Yes. Organisations should list mitigating controls where appropriate to demonstrate the measures they're taking to protect their ICT environments.

Working out how important my information is to determine risk

Organisations decide for themselves what constitutes important information and must record these in an information asset register.

Use of the Office of the Victorian Information Commissioner's (OVIC) Victorian Protective Data Security Framework Business Impact Levels (BILs) may be an appropriate guide.

What can help inform my risk-based decision?

Organisations can use their information asset register to help identify assets suitable for the inclusion.

What is a "position of trust" in multi-factor authentication?

What constitutes a position of trust is unique to each organisation. The Australian Government Information Security Manual – June 2021 (ISM) defines a position of trust as: a position that involves duties that require a higher level of assurance than that provided by normal employment screening.

In some organisations additional screening may be required. Positions of trust can include, but aren't limited to, an organisation's Chief Information Security Officer and their delegates, administrators, or privileged users.

What risk level is set for patching applications / operating systems?

Organisations define their own risk levels for applications and operating systems. See ACSC's guide Assessing Security Vulnerabilities and Applying Patches.