The Cyber Maturity Benchmark is an annual self-assessment of baseline cyber security controls across the Victorian Government.

It's based on the Australian Cyber Security Centre (ACSC)'s **Essential Eight Maturity Model**, last updated in 2021.

What are the benefits of the Benchmark?

According to the ACSC, implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

Completing the Benchmark self-assessment enables agencies to:

- review and understand the maturity of their baseline cyber control strategies
- produce reporting that can be used to make decisions about investment in cyber security improvements
- compare their cyber maturity against a whole-of-government benchmark or selected sectors.

What are the main changes to the Essential Eight maturity model?

The ACSC is committed to providing cyber security advice that is contemporary, contestable and actionable. This includes regular updates to the Essential Eight Maturity Model. The main changes are:

- redefining the number of maturity levels and what they represent.
- moving to a stronger risk-based approach to implementation.
- implementing the mitigation strategies as a package.

For more information see the full ACSC FAQs here.

Where do I go for help?

For Cyber Maturity Benchmark help:

- the Victorian Government Cyber Maturity Benchmark User Instructions provides instructions on how to use the Benchmark self-assessment tool, reporting and benchmarking functionality
- the Improving Cyber Maturity with the Essential Eight guide is a starting point for you to understand how to implement the strategies in your organisation
- the Help section within the Benchmark tool includes a series of articles to help you navigate and use the self-assessment. Access is via Tabs bar > HELP.

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

vmia.vic.gov.au

© Victorian Managed Insurance Authority

VICTORIA State Government

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

D23/418_03-01-2023

- visit the website at www.vmia.vic.gov.au/cyber-maturity-benchmark
- contact VMIA on (03) 9270 6900 or contact@vmia.vic.gov.au

Is the assessment mandatory?

The Cyber Maturity Benchmark is voluntary. Even if you already know your Essential Eight maturity, participating in the assessment contributes to Victoria's Cyber Strategy Mission One: The safe and reliable delivery of government services via the Essential Eight monitoring program. Departments and agencies are strongly encouraged to contribute to the management of this State-significant risk by participating in the Benchmark.

Who is included in the Benchmark?

The Benchmark aims to measure cyber maturity across the whole of Victorian Government. Therefore, all Victorian Government departments and agencies are encouraged to participate.

Selected non-government organisations may be asked to participate due to their connection to government systems or critical infrastructure.

How can I access the Benchmark?

If you've already completed an assessment, you should automatically have access to the self-assessment you've completed. If you're unsure, or are interested in participating in the Benchmark by completing an assessment for the first time, please contact us on (03) 9270 6900 or contact@vmia.vic.gov.au

How does it take to complete the Benchmark self-assessment?

The self-assessment has one question for each of the eight mitigation strategies of the Essential Eight, plus four questions relating to coverage and assurance for each control area.

The timeframe to complete the self-assessment will depend on whether you have the information readily available, or if you need to engage more widely within your organisation.

What level of cyber maturity should I be aiming for?

The ACSC recommends that you implement the Essential Eight in a graduated manner. Your organisation should decide on your current and desired maturity level based on a number of factors including your sector, size, resources, activities, and risk profile.

What do the coverage and assurance sections measure?

In the assessment, coverage refers to the amount of compliant systems covered by the maturity level and your assessment of the risk impact of the non-compliant systems. The assurance section refers to how recently you've had the controls audited; either externally, internally or by a subject-matter expert which could include someone in your organisation with cyber certifications.

What if some of my IT services are provided by a third party?

Managed Service Providers (MSPs), also known as third-party ICT providers, play a key role in the management and supply of ICT for public sector organisations. Understanding which controls are managed by your MSP is part of having a strong working relationship with your MSP and ensuring your organisation is effectively protected. Refer to the "Working with Managed Service Providers" section in the Improving Cyber Maturity with the Essential Eight guide for tips. You can also send your MSP an excel version of the assessment to complete for you available on our website under 'Extra resources'.

How does the benchmarking work?

As soon as a minimum of five agencies in a category have submitted their responses, the benchmarking reports become available. There are a range of filter options for you to compare your agency to others by criteria such as portfolio, sector, budget and number of staff.

If we completed last year, will we still be able to view our results?

Yes, you can still access results from your previous assessment. However, if there's any update to the Essential Eight model, it will not be a direct comparison with the previous year.

We're still working on our improvement plan against the 2020 Essential Eight model. Do we have to re-assess in 2021-22?

The assessment remains optional, however, the updated Essential Eight 2021 aims to keep pace with the threat landscape as well as moving to a stronger risk-based approach to implementation. The 2021-22 assessment will let you know if your organisation is keeping pace against evolving cyber risk.

Can I change or re-take the self-assessment?

You can complete and update your self-assessment as many times as you wish within the Benchmark cycle of each year which ends on 30 September annually.

How does the Essential Eight align with other cyber and information security frameworks?

The Essential Eight contains the technical control strategies to implement part of the Victorian Protective Data Security Standards (VPDSS), Standard 11 – ICT Security. You can certainly use the results of your Essential Eight assessment towards your Standard 11 reporting, but it doesn't replace it.

Additionally, it provides a practical way to implement part of the NIST Cyber Security Framework.

If I have just attested to the VPDSS, do I also need to complete the Cyber Maturity Benchmark?

The information you provide for VPDSS Standard 11 – ICT Security, remains with OVIC and is not used for whole of government cyber benchmarking. Alternatively, the responses you develop for VPDSS Standard 11 can be re-used in the self-assessment for the Cyber Maturity Benchmark. Participating in the Benchmark allows you to compare your organisation against others in the Victorian Public Sector.

Our data and data sharing

How will the benchmarking data be used?

The Cyber Maturity Benchmark data will be used by DPC's Cyber Safety Unit to:

- understand and report on cyber security maturity across the Victorian Public Sector
- make informed decisions about where to invest in improving cyber security across the Government
- develop targeted capability and peer sharing programs to assist agencies to improve cyber security in priority areas
- report to Government on the overall Essential Eight maturity of public sector organisations.

If the Cyber Safety Unit wishes to share your identifiable data with third parties, they will request your permission.

VMIA may use the data from the Benchmark to:

- assist our clients to make informed decisions about cyber risk management
- report de-identified benchmarking results to participating entities
- assist our clients to make informed decisions about cyber risk management
- develop programs, products and services to meet the needs of our clients
- monitor the effectiveness of the Cyber Maturity Benchmark service and other VMIA products and services
- obtain cyber insurance for our clients in the reinsurance market at a competitive price
- fulfil VMIA's obligations under section 23 of the VMIA Act 1996.

VMIA will not use the Benchmark data to calculate individual insurance premiums.

Content is securely stored and the VMIA is bound by Victorian legislation and information management frameworks.

Can other agencies view our results?

No. Your results will be de-identified and included in shared (averaging) benchmarking data and reports made available within the Benchmark tool and in reporting outside the tool.

The benchmarking data and reports are available to other Cyber Maturity Benchmark participants, however, they do not disclose your agency's identity.

Are my results visible to my portfolio department?

The Victorian Cyber Security Unit may use your entity's results when:

- reporting on cyber security maturity in your portfolio
- responding to requests from the department.

If the Cyber Security Unit wishes to share your identifiable data with third parties, they will request your permission.

Can new uses of the data be added in the future?

You will be notified of any future additional uses of the data held in the Cyber Maturity Benchmark before they are implemented.

Can I delete my organisation's data?

Participation in the Cyber Maturity Benchmark is voluntary, and you may delete the data relating to your entity at any time.

Can others in my agency have access to the self-assessment?

Yes, multiple people in your agency can have access to the Benchmark. To learn more about the different user roles, check out the user instructions.

Insurance

How does my self-assessment result affect my VMIA insurance?

VMIA will not use the benchmark data to calculate individual insurance premiums.

We will use aggregated, de-identified data to obtain cyber insurance for our clients in the reinsurance market at a competitive price.

Do I have cyber insurance with VMIA? What does it cover?

VMIA is the Victorian government insurer and risk adviser. For more information about our insurance policies please contact us on (03) 9270 6900 or contact@vmia.vic.gov.au

What is VMIA's role in the Benchmark?

VMIA's purpose is to build a confident, resilient Victoria through world-leading harm prevention and recovery.

Increasingly, our clients are participating in the management of State-significant risks such as cyber. Our role as a strategic adviser is to connect our clients to global best practices and expertise, and to share insights and information with a whole-of-government lens – anticipating future issues and helping our clients to prepare for them.

The Benchmark assists VMIA to:

- develop programs, products and services to meet the needs of our clients
- develop insights to inform risk-based policy and continuous improvement in the Government
- obtain cyber insurance for our clients in the reinsurance market at a competitive price.

What is the role of DPC in this this program?

VMIA has partnered with the Department of Premier and Cabinet's Cyber Safety Unit in Digital Victoria to deliver this program. The Benchmark assists the Victorian Government Chief Information Services Officer (CISO) to:

- understand cyber security maturity across the Government
- make informed decisions about where to invest in improving cyber security across the Government
- develop targeted capability and peer sharing programs to assist agencies to improve cyber security in priority areas.