Victorian Government Cyber Maturity Benchmark

In partnership with the Department of Government Services, Victoria

Interpreting your results

The Cyber Maturity Benchmark is an annual self-assessment of baseline cyber security controls across the Victorian Government. The questions are based on the Australian Cyber Security Centre's (ACSC) **Essential Eight.**

How can I access relevant reports?

- Before you start, check that you have the right data in front of you.
- Log in to the VMIA Self-Assessment Hub and navigate to Assessment Reports to download the report you want:
    › Cyber Maturity Benchmark - Detailed Summary
    › Cyber Maturity Benchmark – Detailed Comparative
    › Cyber Maturity Benchmark – Comparison Summary
    › Cyber Maturity Benchmark – Executive Benchmarking Summary
    › Cyber Maturity Benchmark - Benchmarking Dashboard

    (Note: make sure you select the appropriate Assessment Year)
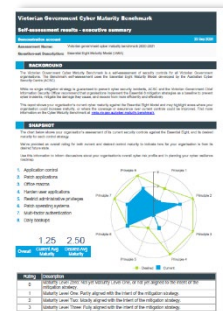
What does the report tell you?

You know your results – and you may have discussed them with your team, colleagues, Board and Executive Management. Your current and desired maturity against the Essential Eight are your core results.

You'll also see an overall score for your averaged current and desired maturity (up to Level 3) across the Essential Eight. Your reports also provide a gap analysis table which demonstrates where you have the largest difference between where you were at the time of the assessment and where you set your desired maturity.

D24/57113

What do the maturity ratings mean?

Your ratings may be well within the range of appropriateness for your size and type of organisation or you might need to do more. The Australian Cyber Security Centre (ACSC) has provided implementation guidance for the Essential Eight model and rated the maturity levels for their broad appropriateness to certain types and sizes of organisations and the data they protect (see Table 1 below).

Table 1: Guidance on which level is appropriate for your organisation

Maturity level	Appropriate for
1	Maturity Level 1 may be suitable for small to medium enterprises with limited sensitive data.
2	Maturity Level 2 may be suitable for medium sized large enterprises.
3	Maturity Level 3 may be suitable for critical infrastructure and service providers, and other organisations that operate in high threat environments.

Cyber maturity isn't a function of size but of purpose and criticality. According to the ACSC, not all organisations need to aim for the highest maturity model, as higher cyber maturity increases the burden on operating environments and isn't appropriate for all organisations.

Where should you start?

The best place to start is by reaching Level 1 across all control strategies before moving on to Level 2.

The ACSC now advises organisations to achieve a consistent maturity level across all Essential Eight control strategies before moving onto a higher maturity level. This is because the Essential Eight strategies are designed to complement each other and to provide broad coverage of various cyber threats.

How do you compare to the baseline?

Using the Benchmarking Dashboard report, you can compare your results against the overall public sector baseline figures for each control strategy, as well as see what the overall average was.

What questions should my organisation be asking?

As well as achieving a baseline measure of public sector cyber maturity in Victoria, the Cyber Maturity Benchmark results have even greater value for the cyber and risk management conversations they ignite.

Here are some questions to pose to your teams, colleagues and Board:

- How do we compare against our peers and the wider baseline?
- Are our results what we expected?
- Are we doing better in this area than we expected?
- How do our results compare to the implementation guidance?
- How are we meeting the needs of our stakeholders? Where could we improve?
- How are we covering (and financing) gaps?
- How can we work (together with others) to improve our cyber security?
- How do our results align to our cyber security strategy, roadmap or plan?
- How well is cyber security integrated into our risk management framework, including risk appetite?

How can I progress the conversation?

It can be challenging if you're one of the only people in your organisation in charge of cyber or risk – but the fact is, just like workplace safety, we're all responsible for contributing to these areas.

Here are some tips:

- How well do you know the people involved in cyber security, risk, and strategy in my organisation, in order to learn more?
- Can you work with your colleagues to advance cyber as an agenda item to showcase your organisations results?
- Seek support from Department of Government Services who can assist with:
  - › Business Case Support Packages with content to help develop business cases to uplift your cyber maturity.
  - › Procurement initiatives available to anyone in the Victorian Government via a panel arrangement, ranging from next generation antivirus software to penetration testing and consulting, password blacklisting, and more.
- Join the Innovation Network's *Whole of Victorian Government Cyber Resilience Network* for regular resources and tips that you can share in your organisation's communication channels.

Want to ask something more specific?

For more information on the Benchmark or to discuss your results, contact us at cyberservice@vmia.vic.gov.au or phone (03) 9270 6900.

For uplift advice and support, including a guide to improve your cyber maturity, see: https://www.vmia.vic.gov.au/cyber-maturity-benchmark