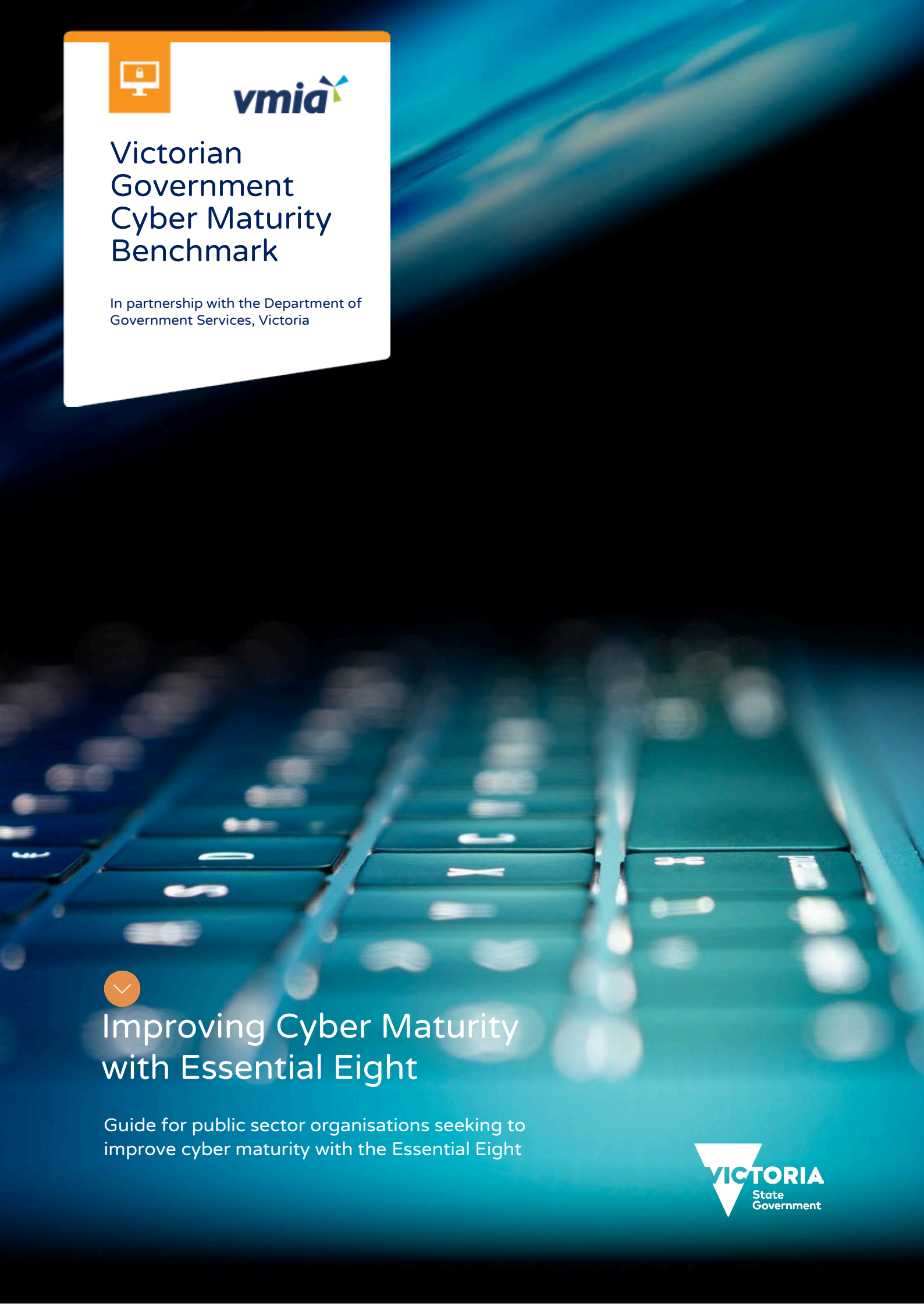


Victorian Government Cyber Maturity Benchmark

In partnership with the Department of Government Services, Victoria

Improving Cyber Maturity with Essential Eight

Guide for public sector organisations seeking to improve cyber maturity with the Essential Eight

Preface

The Victorian Public Sector needs safe, effective and reliable technology to deliver quality services and support Victoria's recovery from the coronavirus pandemic. However, the cyber security maturity of the Victorian Government hasn't kept pace with the scale and sophistication of the attacks we face.

That's why improving cyber security maturity is a priority for everyone.

As risk adviser to the State, VMIA has partnered with the Department of Government Services' (DGS) Cyber Security Unit, to develop the Cyber Maturity Benchmark as an annual measure of cyber control maturity across the Victorian Government.

The Victorian Government supports the use of the Essential Eight Maturity Model, created by the Australian Cyber Security Centre (ACSC) as the baseline of cyber security maturity.

The ACSC Essential Eight Maturity Model was updated in November 2022 to ensure its mitigation strategies evolve with the tactics, techniques and procedures employed by adversaries. We can expect regular updates to the model.

While no single mitigation strategy is guaranteed to prevent cyber security incidents, the Victorian Government Chief Information Security Officer recommend that organisations implement the Essential Eight mitigation strategies as a baseline to prevent cyber incidents, mitigate the damage they cause, and recover from more efficiently and effectively.

About this guide

This guide is a companion to the Victorian Government Cyber Maturity Benchmark, an online self-assessment tool that is hosted on the Victorian Managed Insurance Authority (VMIA) website, see www.vmia.vic.gov.au/cyber-maturity-benchmark.

This guide explains the Essential Eight model, its benefits and limitations, as well as a risk- based approach to implementing a cyber security maturity program. Each control strategy in the model is outlined along with tips and common challenges that an organisation may face in implementation. The guide concludes with suggested next steps for reporting and governance. Note that this guide has been developed to provide public sector risk managers with a foundational understanding of how organisations can undertake Essential Eight uplift activities. It is not intended to be a comprehensive technical guide for ICT managers, or a comprehensive guide to enterprise risk management.

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 Elders past, present, and emerging. We acknowledge the important contribution that Aboriginal and Torres Strait Islander peoples make in creating a thriving Victoria.

D23/81649

Contents

What is the Essential Eight?

Analysis in the Australian Cyber Security Commission's (ACSC) 2021-2022 Annual Cyber Threat Report observes that over the 2021-22 financial year, ACSC received over 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous financial year.[1] In response to this threat, the Essential Eight are a set of technical control strategies targeted at preventing cyber intrusions, ransomware and other malicious events, limit their damage and enable organisations to recover if they occur.

The Essential Eight is a cyber self-assessment (security) maturity tool "to help organisations mitigate cyber security incidents caused by various cyber threats" and have been designed to protect Microsoft Windows-based internet-connected networks.

Developed by the ACSC, the Essential Eight are endorsed by the Victorian Government Chief Information Security Officer (CISO) as being foundational security strategies crucial to managing contemporary cyber security threats.

Analysis by the Cyber Safety Unit's (CSU) Cyber Incident Response Service (CIRS) found that 84% of reported incidents in 2020/21 could have been prevented or significantly minimized by the implementation of at least one of the Essential Eight controls.

To assist organisations in protecting themselves from cyber threats, the Australian Cyber Security Centre (ACSC) developed a three-tier maturity model for the Essential Eight (you'll find the full model in the Appendix).

- Maturity Level Zero: Not yet aligned to the intent of the mitigation strategy (Unofficial)
- Maturity Level One: Partly aligned with the intent of the mitigation strategy
- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy[2]

The Essential Eight is seen as the baseline of cyber security maturity and is just one part of a wider framework that agencies need to have in place.[3]

Cyber resilience is the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.

[1] "ACSC Annual Cyber Threat Report 01 July 2021 to 30 June 2022", ACSC, Sep 22

[2] Essential Eight Maturity Model, ACSC, https://www.cyber.gov.au/acsc/view-all-content/publications/essential- eight-maturity-model

[3] Strategies to Mitigate Cyber Security Incidents, ACSC, https://www.cyber.gov.au/resources-business-and- government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber- security-incidents

Why should public sector organisations measure their maturity against the Essential Eight?

Self-assessing against the model can assist your organisation to:

- increase your knowledge and visibility over your organisation's cyber security
- identify your current application of prioritised technical controls
- identify challenges and opportunities to create a cyber maturity roadmap
- focus on organisational controls rather than users
- inform business cases to secure funding to improve organisational cyber security and resilience
- compare organisational progress against (de-identified) peer sector organisations
- report to executives, audit and risk management committees and boards on cyber security risk
- implement technical controls to support implementation of the Victorian Protective Data Security Standards (VPDSS), ISO27001 and other information security frameworks.

Limitations of the Essential Eight

Whilst implementation of the Essential Eight is increasingly seen as a cornerstone of modern cyber security, it is not a fully-fledged cyber security framework and will not protect organisations from all cyber security threats. Organisations should ensure they appropriately manage the implementation of the Essential Eight with other controls, including uplifting the cyber security knowledge of staff, contractors and volunteers, as part of a cyber or information security best practice aligned framework.

The Essential Eight is principally designed for organisational Microsoft Windows corporate environments, which represent the majority of public sector organisations' corporate environments. Whilst not specifically designed for other ICT environments (e.g. Mac, Cloud, Operational Technology (OT), Linux etc.), the equivalent controls will support organisational cyber security maturity.

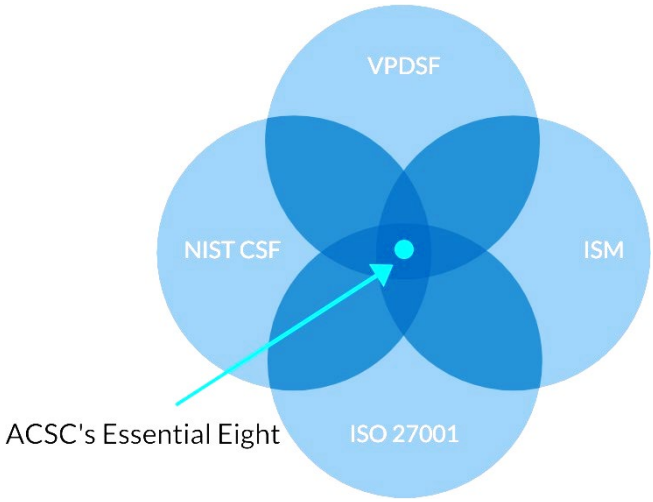
Assurance

A critical component of the Essential Eight is its focus on implementing technical controls which prevent attacks, reduce their impact and aid in the timely recovery from incidents. As public sector organisations' ICT environments are often dynamic and complex, security controls need to be tested to ensure they are implemented, operating as intended haven't led to unintended consequences.

Allocating resources towards engaging an impartial third-party to assure the status of cyber security controls and coverage is recommended. Where third parties or tools cannot be used, internal audit or another internal resource should independently undertake or confirm the results of any assessment.

How does the Essential Eight relate to other programs and assessments?

The Victorian community expect public sector organisations who handle their data, receive public funds or service the community to do so safely and with appropriate controls in place. As cyber threats increase, Victorian public sector organisations commonly utilise best practice frameworks to guide their organisational programs to meet those expectations.



The Essential Eight are foundational security controls common to industry standards

The two key relevant frameworks are summarised below:

Victorian Protective Data Security Framework (VPDSF) 5-Step Program

The VPDSF Five Step Action Plan supports Victorian public sector organisations to implement the VPDSF and meet their obligations under the Privacy and Data Protection Act 2014 (PDP Act 2014). The Five Step Plan supports organisations to structure their information and cyber security programs. Implementing the Essential Eight is aligned to Step 04 - *Applying security measures to protect the information*. The Victorian Information Commissioner and the GCISO endorse using the Five Step Action Plan to improve information security.

Five-Step Action Plan				
01	02	03	04	05
Identify your information assets	Determine the 'value' of this information	Identify any risks to this information	Apply security measures to protect the information	Manage risks across the information cycle

The Five-Step Action Plan

For more information on the Five Step Plan, visit the Office of the Victorian Information Commissioner (OVIC) website.

How does completing the Victorian Government Cyber Maturity Benchmark against the Essential Eight relate to the VPDSS?

You can certainly use the results of your Essential Eight assessment towards your Standard 11 reporting, but it doesn't replace it. The information you provide for *VPDSS Standard 11 – ICT Security* is much broader than the technical focus of the Essential Eight. Alternatively, the responses you develop for VPDSS Standard 11 can be re-used to complete 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. See the Appendix for a table that maps VPDSS Standard 11 with the Essential Eight control strategies.

NIST Cyber Security Framework

To support organisations to treat increasing cyber security risk, in 2013 the United States National Institute of Science and Technology (NIST) released a publicly available Cyber Security Framework (CSF)[4] which has become a globally recognised approach to treat cyber and information security risk. The CSF is a GCISO endorsed approach to uplifting Victorian public sector cyber security maturity, including implementing or improving your Essential Eight Maturity.

The CSF is designed to complement existing organisational processes and operations to provide a comprehensive approach to developing a cyber security program. It is supported by a wide range of freely available resources, and by widespread industry resources. The NIST CSF can be used by organisations in conjunction with the VPDSF and ACSC's Information Security Manual (ISM), including the Essential Eight. There is more on this in Part 3 – Configure Microsoft Office macro settings.

Challenges to improving cyber security maturity

Implementing an effective cyber security program within an organisation comes with similar challenges to implementing any new program, especially when it comes to prioritising resources. Understanding possible barriers will enable you to overcome them as a part of their cyber security improvement strategy. Common challenges voiced by organisations can include:

- We lack the resources (staff and or funding).
- We are not sure that we have the knowledge or skills necessary to successfully implement a cyber maturity program.
- We are often faced with having to prioritise other organisational objectives.
- We have often managed cyber security ad hoc and not as an endorsed project or program of work.
- We can come across resistance when influencing internal stakeholders.
- We've found that some self-assessments can sometimes lead to overestimating maturity and not identifying actions for improvement.

[4] NIST CSF, https://www.nist.gov/cyberframework/framework

Everyone in an organisation has a role to play when it comes to Cyber security – accountability doesn't just fall to the IT Security Manager. To effectively manage cyber risk, Victorian public sector organisations should consider managing their cyber risk through their centrally governed risk management program and cyber security industry best practice. Key cyber security stakeholders to engage with include:

- Chief Executive Officers (CEO) or equivalent
- Chief Risk Officers (CRO) or equivalent
- Board, Executive and Committees
- Chief Information Officers (CIO) or equivalent
- Chief Technology Officers (CTO) or equivalent
- Chief Information Security Officers (CISO)
- System owners and administrators
- Users
- Service providers
- Procurement / Legal counsel
- Finance

Procurement and contract setting

Within your organisation's information security roadmap, you may need to align your procurement and contract setting polices and this can include how you conduct a request for quote (RFQ) or request for proposal (RFP). There are information security risks to consider when conducting a procurement and contracting for good and services, so it's important to consider the following:

- understand the risk of the procurement in terms of access and connections to government services and information
- information security requirements for the lifecycle of the contract
- inserting information security clauses into contract arrangements.[5]

The *Victorian Government Procurement Board* has an information security checklist for contract development in their Information security - goods and services procurement guide. The *Buying for Victoria* site also holds information to assist government buyers about how to ensure that information security is considered during the procurement process and when managing contracts for goods and services.

Working with third-party suppliers

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. Knowing the cyber maturity of your MSPs in relation to the Essential Eight is a part of having a strong working relationship with your MSPs and ensuring your organisation is effectively protected.

Some MSP's may have baseline control strategies for their customer base, and it's worth finding out what these are and assessing if this baseline meets your needs.

Conversely, your organisation may require less stringent controls than the levels set by your MSP. If so, this is also a conversation to have with them.

Whilst most MSPs will be responsive to requests for data (e.g. assessment information) and will support you through the development of a change program, it's also possible to encounter some resistance.

[5] See:https://www.buyingfor.vic.gov.au/information-security-goods-and-services-procurement-guide

To effectively work with MSPs, public sector organisations are encouraged to:

- clearly explain your organisation's intentions and promote cyber security requirements
- practice strong account management practices
- involve MSPs in your project planning (where appropriate)
- require independent assessments and/or unedited assessment reporting to confirm results
- encourage them to become a partner with the ACSC
- work in partnership with MSPs and support them to uplift their security maturity over time.

Improving Essential Eight Maturity

The focus of this section is the practical implementation of each of the Essential Eight controls strategies and the challenges you may face with each control. Although maturity Level 3 is recommended for all controls, as mentioned earlier, this may not be appropriate for the current context of your organisation. If you haven't yet implemented the control, there are suggestions and if you have, there are recommendations on how to increase your maturity as well as tips and quick wins. Each control is also prefaced with an estimation of where it rates in terms of potential user resistance and upfront and ongoing maintenance costs.

Note that organisations should routinely review guidance from the ACSC on how to effectively implement and maintain the Essential Eight via their website.[6]

1. Application control

What is application control?

Application control[7] restricts the use of unauthorised software from being present or running on an ICT system. Application control prevents or restricts the malicious programs that attackers can utilise to breach your network and achieve their objectives within the environment.

Application whitelisting technologies stop malware and other unauthorised software and other unauthorised software from operating and disrupting ICT services. Unlike security technologies such as antivirus software which block identified bad activity and permit all other activity, application whitelisting technologies are designed to only permit known good files and block all others.[8] To be effective, application control should include network endpoints (e.g. workstations) and servers.

Application Control	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Medium	High	Medium

6 https://www.cyber.gov.au/

7 Application control was formally known as application whitelisting. Both terms are used interchangeably within industry guidance and documentation.

8 Guide to Application Whitelisting, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

Rationale

An appropriately configured implementation of application control helps to prevent the undesired execution of software (e.g. Malware) regardless of whether the software was downloaded from a website, clicked on as an email attachment or introduced via CD/DVD/USB.

How it is practically implemented

Application control is implemented using an application control/whitelisting solution (software). Application control is not simply preventing a user from installing new applications to their computer's hard disk.

Challenges

Building on the challenges for cyber security maturity programs previously listed:

- The size and complexity of some organisations can make identifying, listing and maintaining approved software difficult.
- Cloud-based services and tools as forms of shadow ICT can reduce the effectiveness of application control solutions.
- Stakeholders, including users and managers, can push back against being locked into a standard environment. This can include developers, privileged users (e.g. system administrators), researchers and executives.

Uplift

For organisations with no application control solution:

- Review the below references to start the process.
- For basic application control, consider using Windows inbuilt Applocker.[9] Refer to the ACSC hardening guide for further details.[10]
- Consider application control software alternatives suitable for your environment, including reviewing the features of existing antivirus solutions which may offer application control features.

For organisations seeking to increase their maturity:

- Review your existing application control solution for suitability.
- Remove unneeded or unsuitable applications with vulnerabilities from your environment.[11]
- Review temporary rules implemented for development purposes.
- Review user groupings and limit privileged applications to administrators only.

[9] AppLocker, Microsoft, https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender- application-control/applocker/applocker-overview

[10] Hardening Microsoft Windows 10 version 21H1 Workstations, ACSC, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations

[11] See https://nvd.nist.gov/vuln/search to identify known vulnerabilities in organisational software.

Tips and quick wins

- Maintain next generation anti-virus solutions when application control is implemented.
- Plan application deployment, engaging stakeholders to ensure they identify their applications from critical to nice-to-have.
- In environments with varied applications needs, consider allowing all current existing applications, and filter down over time with extensive stakeholder engagement.
- Simplify your request process for software whitelisting to reduce stakeholder resistance.
- Conduct regular maintenance with stakeholder groups to ensure lists remain accurate, and new application needs are being met.
- Use existing application whitelisting templates to help establish a baseline[1] before you customise to meet your organisation's needs.
- When procuring whitelisting solutions, consider service implementation and maintenance support as part of your procurement activity.

References

- Implementing Application Control, ASCS, https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control
- Guide to Application Whitelisting, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf
- Application Control for Windows, Microsoft, https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

2. Patch application

What is 'patching applications'?

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. 'Patching applications' is the systematic implementation of software updates to ensure functionality and security updates/fixes are applied to applications within your ICT environment. Patching applications prevents attackers from using known security vulnerabilities to breach your network and achieve their objectives.

Patching Applications	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Patch applications (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' security vulnerabilities within 48 hours. Use the latest version of applications. **Flash was end of Life on 01/01/2021	Low	High	High

Rationale

A risk-based approach to patching applications used by organisations keeps security up to date before known vulnerabilities can be exploited by commonly available tools (e.g. exploits).

How it's practically implemented

Patching applications is achieved through the updating of system software in a systematic and prioritised approach. It can be achieved through:

- software which automatically updates
- centralised management operating system tools initiating patching
- third-party patching management tools
- users being prompted to manually update their software.[12]

Challenges

Building on those previously listed, challenges for cyber security maturity programs include:

- Identifying current organisation ICT assets and patching baseline.
- Patching can interrupt system functionality in environments where high availability is required.
- Balancing deploying and testing patches versus. having effective security of high-risk assets.
- Legacy ICT infrastructure may no longer have patches released for known vulnerabilities.
- Bring Your Own Devices (BYOD) and requiring users to update their software.
- Maintaining patching can be manpower intensive.
- Validation and verification patches correctly installed on the device.
- Although upgrading within 48 hrs is a positive, updates are frequently released with faults and errors which take extra time to work through and wait for the fixes.

Uplift

For organisations with no patch management program, review the below references to start the process. For organisations seeking to increase their maturity:

- centrally identify and resource risk-based patching on devices
- use vulnerability scanners on networks
- manually review patches on high-risk devices and applications
- remove legacy devices and applications.

[12] Users being prompted to manually update software is not recommended by the GCISO without further patching automation.

Tips and quick wins

- Review current patching processes for opportunities to improve.
- Prioritise applications vulnerable to exploitation in accordance with industry guidelines.
- Patching policies should be centrally managed by risk committees.
- Remove legacy devices and programs from the network.
- Segregate legacy software unable to be removed from the corporate environment.
- Use patch management systems to monitor organisational patching levels.
- Identify the end-of-life applications (those that suppliers aren't providing updates for) and plan to remove or replace them.
- Apply firmware patches, including for network devices such as remote access solutions, routers, switches and firewalls, and especially for any device that is connected to the internet.

References

- Assessing Security Vulnerabilities and Applying Patches, ACSC, https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities- and-applying-patches
- Guide to Enterprise Patch Management Technologies, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

3. Configure Microsoft Office macro settings

What is Configure Microsoft Office macro settings?

Microsoft Office applications commonly used across the Victorian public sector can execute macros to automate routine tasks. Macros are popular applications which can enable highly efficient repetitive processes. However, macros can contain malicious code resulting in unauthorised access to sensitive information as part of a targeted cyber intrusion, including being used to download other malicious software.

Microsoft Office environments can be configured to prevent macros which have come from the internet or have not been identified as trusted.

Configure Microsoft Office Macro Settings	Potential User Resistance	Upfront Cost (staff, software, and hardware)	Ongoing Maintenance Cost
Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	Medium	Medium	Medium

Rationale

Microsoft Office can be configured to prevent macros from being used to run or download undesirable software (e.g. Malware). Furthermore, preventing untrusted macros from running reduces the risk of staff inadvertently authorising macros to run on their machine.

How it's practically implemented

Configuring Microsoft Office macro settings can be done through the internal security features of Microsoft Office[13] or group policy configuration.

Challenges

Building on the challenges for cyber security maturity programs previously listed:

- Macros are often highly popular applications. Reconfiguring organisational process can cause resistance.
- Organisations often lack the technical capability to effectively analyse macros to identify if they should/should not be trusted.

Uplift

For organisations with no Microsoft Office macro configuration:

- Review the below references to commence the process.
- Engage users to identify macro use.
- Configure Microsoft Office group policies.
- For organisations seeking to increase their maturity:
- Review macro use in the organisation, identify use cases and stakeholders.
- Develop the technical capability to review macros, including tools.
- Establish organisational policies to guide macro screening.

[13] Enable or disable macros in Office files, Microsoft, https://support.microsoft.com/en-us/office/enable-or-disable-macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

Tips and quick wins

- Enforce the macro security configuration settings via your organisation's group policy to prevent users from changing security settings to run a malicious or otherwise unapproved macro.
- Change configurations, engaging stakeholders (e.g., finance and other heavy data users) to ensure they identify and prioritise their macro needs, from critical to nice-to-have.
- Simplify your macro request process to reduce stakeholder resistance.

References

- Microsoft Office Macro Security, ACSC, https://www.cyber.gov.au/resources- business-and-government/maintaining-devices-and-systems/system-hardening- and-administration/system-hardening/microsoft-office-macro-security
- Intel Insight: How to Disable Macros, CIS Security, https://www.cisecurity.org/ white-papers/intel-insight-how-to-disable-macros

4. User application hardening

What is user application hardening?

User application hardening reduces the 'attack surface' malicious cyber actors can use to deploy malicious software onto user systems (e.g. workstations). Blocking or removing common software used to download or run malicious software prevents malicious software from running on organisation networks and disrupting ICT services.

User Application Hardening	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE – Object linking and embedding), web browsers and PDF viewers.	Medium	Medium	Medium

Rationale

Appropriately configured applications help prevent undesired execution of software (e.g. Malware) being downloaded from a website, an email attachment or being introduced via CD/DVD/USB. Furthermore, it reduces the software which attackers can utilise to attack your environment.

How it's practically implemented

User application hardening is achieved through configuring user environment applications and the removal of unwanted or unnecessary applications. This can be achieved through using group policy administrative templates.[14]

Challenges

Building on those previously listed, challenges for cyber security maturity programs include:

- User functionality can be reduced when hardening workstations, this can result in resistance.
- Removing software could impact on necessary organisational workflows.

Uplift

For organisations with no application hardening:

- Review the below references to commence the process.
- Identify where the organisation uses Flash and Java.
- Configure browsers to block Flash content.
- Test changes with user groups.[15]

For organisations seeking to increase their maturity:

- Configure firewalls to block web advertisements and Java from the internet.
- Configure Office to prevent activation of Object Linking and Embedding packages.

Tips and quick wins

- Utilise group policy administrative templates to implement changes across network environments.
- Conduct regular maintenance with user groups to ensure your use case lists remain accurate.

References

- Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016, ACSC, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices- and-systems/system-hardening-and-administration/system-hardening/hardening- microsoft-365-office-2021-office-2019-and-office-2016
- Hardening Microsoft Windows 10 version 21H1 Workstations, ACSC, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices- and-systems/system-hardening-and-administration/system-hardening/hardening- microsoft-windows-10-version-21h1-workstations

[14] Administrative templates are a feature of Group Policy, a Microsoft technology for centralised management of systems using a Microsoft environment.

[15] Preventing Flash and Java web applications may prevent web applications, such as training and administrative portals, from functioning.

5. Restrict administrative privileges

What is restricting administrative privileges?

User accounts with administrative privileges for operations systems and applications can make significant changes to workstations and network configurations, bypass security settings and access, modify or delete sensitive information. Higher level administrators, such as domain administrators, have similar ability on entire networks.

When attackers have access to accounts with administrator privileges, they can access more computer and system resources than regular users. This can occur when an administrator's account is breached or a regular user account's privileges are escalated to those of an administrator.

Restricting administrator privileges does not seek to prevent legitimate administrator activity but introduce safeguards to prevent account misuse. Restricting administrator privileges can also prevent unintentional changes to network environments. To be effective, all administrators accounts must have restrictions placed on their use.

Restrict Administrative Privileges	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	Medium	High	Medium

Rationale

The consequences of a compromise can be reduced if a user account (the attacker) does not have administrative privileges.

How it's practically implemented

Restricting administrator privileges is achieved through the implementation of a range of measures, including:

- amending organisational business practices for administrators
- configuration changes to network devices
- purchasing dedicated devices and/or software solutions.
- Simply minimising the total number of privileged accounts can increase risks to an organisation's network, so we recommend organisations take an approach aligned to industry best practice.

Challenges

Building on those previously listed, challenges for cyber security maturity programs include:

- changing administrator behaviour and overcoming resistance
- overcoming user resistance to remove administrator privileges.

Uplift

For organisations with no restrictions on administrator account uses:

- review the below references to commence the process
- remove unused administrator accounts
- ensure all default log in credentials have been changed
- define who in the organisations should be a privileged user and what type of privileges they should have
- configure environment to prevent privileged accounts from accessing email and the internet.

For organisations seeking to increase their maturity:

- establish privileged access review process and policies to revalidate access
- harden environment to further protect administrator accounts.

Tips and quick wins

- Review current administrative processes for opportunities to improve.
- Undertake a staged roadmap approach to securing administrator accounts.
- Engage users with administrative access to understand use cases and implement new business processes.
- Undertake a discovery stage and reduce access over time.
- Use dedicated workstations for administrator accounts.
- Consider privileged access management solutions.

References

- Restricting Administrative Privileges, ACSC, https://www.cyber.gov.au/acsc/view-all-content/publications/restricting-administrative-privileges
- Implementing the Critical Security Control: Controlled Use of Administrative Privileges, SANS Institute, https://www.sans.org/reading-room/whitepapers/critical/implementing-critical-security- control-controlled-administrative-privileges-37115
- Implementing Least-Privilege Administrative Models, Microsoft, https://docs.microsoft.com/en- us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege- administrative-models
- Securing privileged access for hybrid and cloud deployments in Azure AD, ACSC, https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin- roles-secure

6. Patch operating systems

What is patching operating systems?

Patching operating systems is the process of keeping our workstations and servers up to date with the latest technologies to improve security, functionality, reliability and user experience. Updating operating systems, like patching applications, is the systematic implementation of software updates to ensure functionality and security updates/fixes are applied to your ICT environment. Patching operating systems prevents attackers from using known security vulnerabilities to attack your network devices and achieve their objectives.

Patching Operating Systems	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' security vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.	Low	Medium	Medium

Rationale

A risk-based approach to patching operating systems used by organisations keeps security up to date before known vulnerabilities can be exploited by commonly available tools (e.g. exploits).

How it's practically implemented

Patching operating systems is achieved through the updating of system software in a systematic and prioritised approach. It can be achieved through:

- software which automatically updates
- centralised management operating system tools initiating patching
- third-party patching management tools
- users being prompted to manually update their software.[16]

Challenges

Building on those previously listed, challenges for cyber security maturity programs include:

- identifying current organisation ICT assets and patching baseline
- patching can interrupt system functionality in environments where high availability is required
- balancing deploying and testing patches vs. having effective security of high-risk assets
- legacy ICT infrastructure may no longer be patched, or only have patches available from a third party
- bring Your Own Devices (BYOD) and requiring users to update their software
- maintaining patching can be manpower intensive
- validation and verification patches correctly installed on the device.

[16] Users being prompted to manually update software is not recommended by the GCISO without further patching automation.

Uplift

For organisations with no patching strategy:

- review the below references to commence the process
- establish central oversight of patching through developing a patching strategy and vulnerability management plan
- remove unsupported legacy devices and operating systems from the network.

For organisations seeking to increase their maturity:

- use vulnerability scanners on networks
- manually review high-risk devices
- employ patch management technologies and processes to deploy patches within risk-based timeframes.

Tips and quick wins

- Review current patching processes for opportunities to improve.
- Identify the end-of-life applications (those that suppliers aren't providing updates for) and plan removal and replacement from the environment.
- Following industry guidelines, prioritise operating systems that are vulnerable to exploitation.
- Patching policies should be centrally managed by risk committees.
- Remove legacy devices from the network.
- Segregate legacy operating systems which can't be removed from the corporate environment.

References

- Assessing Security Vulnerabilities and Applying Patches, ACSC, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-administration/assessing-security-vulnerabilities-and-applying-patches
- Guide to Enterprise Patch Management Technologies, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

7. Multi-factor authentication

What is multi-factor authentication?

Multi-factor authentication is one of the most effective security measures organisations can implement to prevent attackers from gaining access to networks and devices. Often known as two- factor authentication, multi-factor authentication requires users to present two or more separate pieces of evidence when signing into their account. For example, two or more of the following:

- username and password – something you *know*
- authorisation through an MFA (multifactor authentication) application – something you *have*
- your fingerprint – something you *are*.

Practical example: Requiring a bankcard (something you have) and pin (something you know) to complete a purchase.

What is the two-factor authentication? Source: ACSC

Multi-factor authentication prevents attackers from gaining access to accounts if they guess the password or know the username and password. Multi-factor authentication should be implemented for all remote access, high privileged accounts (e.g. administrators) and when users require access to important data.

Multi-factor Authentication	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high- availability) data repository.	Medium	High	Medium

Rationale

Increasing the strength of user authentication makes it harder for attackers to gain access to sensitive systems and information. When implemented correctly, multi-factor authentication makes it significantly more difficult for attackers to gain access to legitimate accounts (e.g. through phishing) to steal credentials and undertake further malicious attacks on systems.

How it's practically implemented

Implementing multi-factor authentication will depend on the ICT environment within your organisation and the multi-factor authentication method you select.

However, it will commonly occur via:

- Configuration of network authentication systems (e.g. Windows activity directory).
- Selection and introduction of a multifactor authentication technology (e.g. an authenticator phone application or token).

Challenges

Building on the challenges previously listed, challenges for cyber security maturity programs include:

- Users, in particular executives and administrators (who often manage multiple accounts), can resist multi-factor authentication.
- Legacy systems may not supply multi-factor authentication.

Uplift

For organisations with no multi-factor authentication systems:

- Review the information in the references section below to commence the process.
- Establish a project to identify, select and implement multi-factor authentication.

For organisations seeking to increase their maturity:

- Require multi-factor authentication for all users.
- Employ secure multi-factor authentication technology.

Tips and quick wins

- Select multi-factor authentication solutions which provide increased protection with less friction to reduce user resistance.
- Turn off legacy authentication to prevent bypass.
- If possible, use multi-factor authentication policies and settings to reduce user friction.
- Undertake a staged roadmap approach to deploying multi-factor authentication across your network, starting with high-risk accounts.
- Consider trialling multi-factor authentication with volunteers within user groups to learn lessons.
- Engage users to understand the new requirements and processes.
- When enforcing multi-factor authentication, have a support plan to handle failed logins, account lockouts and users unable to access their accounts.
- Remove legacy devices and programs which don't support multi-factor authentication from the network.

References

- Implementing Multi-Factor Authentication, ACSC, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication
- Configure Additional Authentication Methods for AD FS, Microsoft, https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-additional-authentication-methods-for-ad-fs

8. Daily backups

What are daily backups?

Backups of important or new information and software are a means to restore operating systems quickly following a service disruption. Critically, backups must be tested to make sure they're functioning correctly, and organisations have processes to effectively recover the data they need.

Attackers commonly target backups, so storing backup data 'offline', where backups can't be accessed or written over is increasingly important.

As more government services move online, daily backups are becoming increasingly important, as critical data needs to be retained so that if a cyber incident does occur, service disruption is minimal. As a result, organisations may require hourly or continuous backups.

Daily Backups	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	Low	High	High

Rationale

Regular backups can be used to access information following a cyber incident (such as a ransomware incident), and mitigate attacks which might encrypt, modify or delete data.

How it's practically implemented

You can implement daily backups by:

- defining organisational backup requirements, including security of backups
- selecting a storage solution or vendor which meets organisational requirements
- configuring systems to enable backup
- testing restoration capability
- fully developing backup and restoration procedures.

Challenges

Cloud storage has significantly reduced the challenges and costs associated with backing up data. Building on those previously listed, challenges for cyber security maturity programs include:

- ensuring the security of backups in cloud environments
- protecting backups from ransomware
- proving capability to restore from backups
- demonstrating 'value for money' for security control.

Uplift

Organisations with no backup process should:

- review the below references to commence the process
- establish a backup and restoration policy
- identify important business data
- implement technologies and procures to backup data to desired maturity level
- test restoration of backups.

Organisations that want to increase their maturity should review policies and procures against the maturity model for opportunities to improve.

Tips and quick wins

- Review backup procedures to identify areas to improve.
- Ensure data recovery is embedded in business continuity planning and testing.

References

- Contingency Planning Guide for Federal Information Systems, NIST, https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

Following the assessment

If you're using the Essential Eight model to assess your organisation's maturity, it's unlikely you'll rate a maturity level 3 for all strategies.

The ACSC recommends a maturity level 3 for all organisations, but an organisation's optimum maturity level depends on its business need, size and operational complexity.

We recommend organisations look at the adequacy of their cyber security strategy, policies, procedures and protections after they've completed the assessment.

The National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) explains the steps an organisation can take to implement the Essential Eight.

The NIST CSF provides an industry best practice guide to improve cyber security maturity, including implementing or improving Essential Eight maturity

Steps 3 to 7 of the cycle above will be particularly useful for public sector organisations moving between maturity levels of the Essential Eight:

- Step 3: Create a current profile
  - Creating a current profile identifies the status of the organisational cyber security controls. This allows organisations to understand where they sit in the Essential Eight.
- Step 4: Conduct a risk assessment
  - Assessing the organisation's risk profile, including incorporating emerging risks, threats and vulnerabilities, helps organisations understand where they are exposed to risk and supports later steps.

- Step 5: Creating a target profile
  - This involves identifying and defining what controls the organisation needs. Using the Essential Eight as a basis for a target profile will help improve maturity.
- Step 6: Determine, analyse and prioritise gaps
  - Comparing the current and target profiles will help organisations determine gaps and create an action plan that incorporates risk management needs, organisational drivers and available resources.
- Step 7: Implement action plan
  - Once prioritised, organisations select and implement their action plan to achieve their target profile.

Taking these steps will help your organisation prepare and address exposures to risk.

Prioritising uplift programs

The level of protection required will depend on your organisational circumstances. However, organisations are encouraged to:

- take steps to adequately understand the technical risks
- update organisational risk assessments (if applicable)
- review their cyber security strategy, policies, procedures and protection in place
- communicate and report findings to oversight bodies with accompanying recommendations.

Tips and quick wins

Organisations may find it beneficial to form cyber security steering committees, drawing appropriate representation from stakeholders, to work through a planned uplift program.

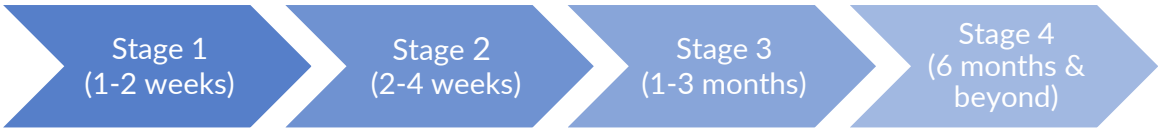
If your organisation plans to run a cyber maturity uplift program, proposed changes should be prioritised in the context of organisational requirements.

The following factors might influence your prioritisation efforts:

- short, medium and long-term business and ICT goals and strategies
- available quick wins
- existing threats to organisational information assets
- emerging threats to organisational information assets
- legacy ICT infrastructure
- existing contracts with suppliers
- risk assessment results and current mitigating controls
- stakeholder resistance
- available resources.

Security roadmap

Establishing a staged security roadmap will help your organisation improve the way it implements the Essential Eight. Depending on your organisation's current Essential Eight profile, improvements may be possible immediately, where others will need a longer project delivery timeframe. A roadmap supports prioritisation and good cyber security program governance.



Developing a staged security roadmap will help organisations improve maturity

Appendix A

Standard 11 – Information Communications Technology (ICT) Security

Standard

An organisation establishes, implements and maintains Information Communications Technology (ICT) security controls.

Statement of objective

To maintain a secure environment by protecting the organisation's public sector information through ICT security controls.

Elements

V2.0 #	V1.1 #	Element	Primary Source	Essential 8 Link
E11.010	ICT- 010	The organisation manages security documentation for its ICT systems (e.g., system security plans).	Australian Government Information Security Manual (ISM) • Guidelines for security documentation	
E11.020	ICT- 020	The organisation manages all ICT assets (e.g., on-site and off-site) throughout their lifecycle.	ISM • Guidelines for physical security • Guidelines for ICT equipment management	
E11.030	ICT- 040	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing or storing public sector information.	ISM • Guidelines for authorising systems	
E11.040	ICT- 050	The organisation undertakes risk- prioritised vulnerability management activities (e.g. patch management, penetration testing, continuous monitoring systems).	ISM • Guidelines for system monitoring	Patch Applications Patch operating systems
E11.050	ICT- 060	The organisation documents and manages changes to ICT systems.	ISM • Guidelines for system management –	

V2.0 #	V1.1 #	Element	Primary Source	Essential 8 Link
			Change management	
E11.060	ICT- 070	The organisation manages communications security controls (e.g., cabling, telephony, radio, wireless networks).	ISM • Guidelines for communications infrastructure • Guidelines for communications systems • Guidelines for network management – wireless networks • Guidelines for physical security – wireless devices and radio frequency transmitters	
E11.070	ICT- 080	The organisation verifies the vendors security claims before implementing security technologies.	ISM • Guidelines for evaluated products	
E11.080	ICT- 090	The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.	ISM • Guidelines for media management	
E11.090	ICT- 100	The organisation manages standard operating environments (SOEs) for all ICT assets, including end user access devices (workstations, mobile phones, laptops), network infrastructure, servers and Internet of Things (IoT) commensurate with security risk.	ISM • Guidelines for system hardening	Application Control Configure macros User application hardening Multi-factor authentication
E11.100	ICT- 110	The organisation manages security measures for email systems.	ISM • Guidelines for email management	
E11.110	ICT- 120	The organisation logs system events and actively monitors these to detect potential	ISM • Guidelines for	

V2.0 #	V1.1 #	Element	Primary Source	Essential 8 Link
		security issues (e.g., intrusion detection/prevention systems (IDS/IPS)).	system monitoring	
E11.120	ICT- 130	The organisation uses secure system administration practices.	ISM • Guidelines for system management • Guidelines for personnel security - Privileged access to systems	Restrict administrative privileges
E11.130	ICT- 140	The organisation designs and configures the ICT network in a secure manner (e.g., segmentation, segregation, traffic management, default accounts).	ISM • Guidelines for network management	
E11.140	ICT- 160	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).	AS ISO/IEC 27002:2015 Code of practice for information security controls • 10.1.2	
E11.150	ICT- 150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation and authentication commensurate with the risk to information.	ISM • Guidelines for using cryptography	
E11.160	ICT- 170	The organisation manages malware prevention and detection software for ICT systems.	ISM • Guidelines for gateway management • Guidelines for data transfers and content filtering	
E11.170	ICT- 190	The organisation segregates emerging systems from production systems (e.g., physical and/or logical) until their security controls are validated.	ISM • Guidelines for software development	

V2.0 #	V1.1 #	Element	Primary Source	Essential 8 Link
E11.180	ICT- 200	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).	ISM • Guidelines for system management	Daily backups
E11.190	ICT- 210	The organisation manages a secure development lifecycle covering all development activities (e.g. software, web-based applications, operational technology (Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS)).	ISM • Guidelines for software development	
E11.200	–	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).	ISM • Guidelines for enterprise mobility AS ISO/IEC 27002:2015 • 6.2 PSPF PHYSEC-15 Physical security for entity resources • C.8	Multi-factor authentication