



PC COMPUTING
— & CONSULTING —

ESSENTIAL EIGHT COMPLIANCE SELF-ASSESSMENT



CHECKLIST

ESSENTIAL EIGHT COMPLIANCE SELF-ASSESSMENT CHECKLIST

This checklist is provided to help you evaluate your company's compliance with industry standards and regulations.

Achieving compliance is crucial for safeguarding your business against cyber threats and ensuring data security.









In this checklist, we will cover the eight essential areas of compliance that every company should focus on. Take a few minutes to assess your current practices in each area to identify areas for improvement.

FIRSTLY, WHAT IS THE ESSENTIAL EIGHT?

The Australian Cyber Security Centre (ACSC) recommends eight essential strategies for preventing malware delivery, limiting the impact of cybersecurity attacks, and improving recovery.

The Australian Signals Directorate has stated that implementing the Top 4 mitigation strategies can prevent up to 85% of unauthorised intrusions. The Essential Eight strategies themselves cover vital areas of concern for many organisations.

These include:

Prevent Attacks	 Application Whitelisting	 Patch Applications	 Configure Microsoft Office	 User Application Hardening
Limit Attack Impact	 Restrict Administrative Privileges	 Patch Operating Systems	 Multi-Factor Authentication	
Data Availability	 Daily Backups			



Want to learn more?

[Start Learning](#)



SECTION 1

ARE YOU WHITELISTING APPLICATIONS?

Why this is vital:

Protects your systems by allowing only approved software, reducing the risk of malware attacks.

- We maintain an up-to-date list of approved applications.
 - Only authorised applications are allowed to run on our systems.
 - Regular reviews and updates of the whitelist are conducted.
-

SECTION 2

ARE YOU PATCHING YOUR APPLICATIONS REGULARLY?

Why this is vital:

Closes security gaps, making it difficult for hackers to exploit vulnerabilities in your software.

- We have a documented process for applying patches.
 - Critical patches are applied promptly upon release.
 - A patch management schedule is maintained and followed.
-

SECTION 3

HAVE YOU CONFIGURED MICROSOFT OFFICE SAFELY?

Why this is vital:

Ensures safe document handling, shielding you from malicious files and cyber threats.

- Microsoft Office settings are configured securely.
 - Employees are educated about Microsoft Office security best practices.
 - Macros from untrusted sources are restricted.
-

SECTION 4

IS YOUR USER APPLICATION HARDENING EFFECTIVE?

Why this is vital:

Strengthens user software, preventing unauthorised access attempts and data breaches.

- User applications are configured with security in mind.
- Regular security updates for user applications are applied.
- Monitoring and control measures for user application security are in place.



SECTION 5

ARE ADMINISTRATIVE PRIVILEGES PROPERLY RESTRICTED?

Why this is vital:

Reduces insider threats and unauthorised system changes, enhancing overall security.

- We adhere to the principle of least privilege.
 - Regular reviews of user privileges are conducted.
 - Controls and monitoring of privilege escalation are implemented.
-

SECTION 6

ARE YOUR OPERATING SYSTEMS ADEQUATELY PATCHED?

Why this is vital:

Fixes known vulnerabilities, safeguarding your entire system from potential attacks.

- We have a documented process for applying operating system patches.
 - Critical operating system patches are applied promptly.
 - A patch management schedule for operating systems is maintained.
-

SECTION 7

IS MULTI-FACTOR AUTHENTICATION IN PLACE?

Why this is vital:

Adds an extra layer of security, making it significantly harder for hackers to breach your accounts.

- Multi-factor authentication is enabled for critical systems and accounts.
 - Users are educated on MFA usage and best practices.
 - Regular MFA audits and reviews are conducted.
-

SECTION 8

DO YOU PERFORM DAILY BACKUPS?

Why this is vital:

Guarantees data recovery after loss, ensuring business continuity and safeguarding against data disasters.

- Daily data backups are performed.
- Backup data is securely stored, both on-site and off-site.
- Regular testing of backup restoration is conducted to ensure data integrity.



WHAT IS MY ORGANISATION'S ESSENTIAL EIGHT MATURITY LEVEL?

Determining your organisation's Essential Eight maturity level is crucial for effective cybersecurity. By aligning your strategy with your risk profile, you can optimise security measures while minimising disruption.

ASSESSMENT FOR TAILORED COMPLIANCE

Different businesses have unique compliance needs. The most straightforward way to gauge your compliance path is through a professional Essential Eight maturity level assessment. This comprehensive evaluation involves a risk audit and a cybersecurity audit conducted simultaneously.

BEYOND THE ESSENTIALS

While the Essential Eight provides a foundational security standard, your specific environment may require additional measures. It's essential to consider these unique needs in your compliance journey.

To enhance your cybersecurity posture and advance to the next maturity level, you must identify and address specific risks, estimate associated costs, and assess potential consequences of non-compliance.

SECURE YOUR DIGITAL FUTURE WITH PCC: YOUR ESSENTIAL EIGHT PARTNER

Security in the digital age is non-negotiable. The Essential Eight framework equips your company with the tools to shield against modern cyber threats. By assessing your Essential Eight maturity level and customizing your security measures, you can bolster your companies resilience.

PCC is your dedicated partner throughout this process. Whether you need an assessment, professional advice, or end-to-end support, we're here to guide you. Connect with us, and let's embark on the journey to Essential Eight readiness, ensuring your digital assets remain protected.



Book a Free Consultation

