Marsh

Marsh Advisory | Cyber Risk Consulting

ASD Essential 8 Assessment

For federal agencies and public sector organisations

Validate, uplift cyber maturity and demonstrate compliance to mandated federal government requirements.

The advancement of digitalisation has been a key driver towards organisational efficiency. The scale in which cyber operates has conversely led to rapid increases in both the volume and sophistication of cyberattacks.

As a key element of critical infrastructure, government and public sector organisations are a primary target for cyber criminals. Adversaries are continuously exploiting weaknesses in IT security and information management systems through practices such as targeted phishing emails and ransomware attacks.

What is the ASD Essential 8?

The Australian Cyber Security Centre (ACSC) based within the Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the **Essential Eight**. All organisations, public and private in Australia are encouraged to implement Essential 8. For NSW Government agencies, implementing Essential 8 is a policy imperative. Under the NSW Cyber Security Policy (CSP), each agency must implement Essential 8 as well as annually report a maturity assessment against Essential 8.

Created in February 2017, the Australian Signals Directorate (ASD) found that when operating effectively, the Essential 8 mitigates 85% of targeted cyber-attacks.

Marsh's ASD Essential 8 Assessment can help you achieve and improve your Essential 8 compliance.

WHAT ARE THE ASD ESSENTIAL 8 SECURITY CONTROLS?

The ASD considers Essential 8 to be the most effective cyber resilience 'baseline' for Australian organisations.

The 8 controls are:

Application Whitelisting: To control the execution of unauthorized software

Configure Macros: To block untrusted macros

Multi-Factor Authentication: To protect against risky activities

Restrict Admin Permissions: To limit powerful access to systems

Patching Applications: To remediate known security vulnerabilities

Application Hardening: To protect against vulnerable functionalities

Patch Operating Systems: To remediate known security vulnerabilities

Daily Backups: To maintain availability of critical data

HOW IT WORKS

The ASD Essential 8 Assessment is split into three stages:

Step 1
Marsh Cyber Advisory provide a self-assessment survey on the different maturity levels of the Essential 8 controls. Our Cyber Consultants conduct workshops with you, in order to respond and validate as accurately as possible. All evidence is reviewed to determine the extent of controls implemented.

Step 2
With the captured responses a score is assigned and mapped to an ASD Essential 8 maturity level. Once all the responses are collated an overall maturity level is established.

Step 3
Control gaps are then identified and recommendations provided to uplift to a baseline.

Step 4
All the information is pulled together into a report and presented to stakeholders.

In addition to this report our team are also able support in implementation of additional controls, if required.

Minimise cyber risk and exposure

By undertaking this assessment your organisation will not only validate your current cyber security practices and identify any potential gaps, it will also uplift your cyber maturity posture in line with Australian government guidance – minimising your cyber risk and likelihood of exposure.

Key Contact

Marsh Advisory | Cyber Risk Consulting

For more information about how you can benefit from our services, please contact your Marsh Risk Advisor.

Gill Collins
Head, Cyber Incident Management and Cyber Consulting, Pacific
+61 499 364 283
gill.collins@marsh.com

Steve Thompson
Senior Manager, Cyber Solutions – Marsh Advisory, APAC
+61 467 958 546
steve.thompson@marsh.com

BENEFITS

Validate current cybersecurity practices. and identify any potential gaps.

Demonstrate compliance with mandated federal government requirements.

Uplift cyber insurability profile and cyber maturity posture.

WHY MARSH

As experts in enterprise and cyber risk, we help you take an enterprise wide, scalable approach in building your cyber resilience.

Together, we identify your risks, and develop a best-for-you program and team of partners to help manage it.

Informing your approach and decision-making process with our 25 years of cyber expertise and data-driven insight.

So that your path to cyber resilience is more productive and predictive; and your outcomes are more efficient and effective.

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 45,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people.

With annual revenue over $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.