NIST FRAMEWORK GAP ANALYSIS

Siege Cyber offers comprehensive **NIST Cybersecurity Framework (CSF)** assessments and gap analyses to help Australian companies enhance their cybersecurity maturity.

Our services provide a structured approach to identifying and mitigating security risks, ensuring your company adheres to best practices and regulatory requirements.

We are proud to be an official Network Partner of the Australian Cyber Security Centre (ACSC).

INITIAL CONSULTATION

Understand your business environment and unique cybersecurity needs:

- ✓ Discuss the current cybersecurity posture.
- ✓ Identify critical assets and data.
- ✓ Understand business goals and regulatory requirements.
- ✓ Define the scope of the assessment.

NIST FRAMEWORK GAP ANALYSIS

Identify gaps between the current security posture and the NIST Cybersecurity Framework (CSF):

Current State Review:

- ✓ Evaluate existing technologies.
- ✓ Review security policies and procedures.
- ✓ Identify critical assets and their protection status.

NIST CSF Mapping:

- ✓ Map existing controls to the NIST CSF.
- ✓ Identify gaps and areas needing improvement.
- ✓ Prioritise gaps based on risk and impact.

CYBERSECURITY NIST FRAMEWORK ASSESSMENT

Perform a thorough assessment of the cybersecurity posture using the NIST CSF:

Identify (ID):

- ✓ Asset Management: Inventory of hardware, software, and data.
- ✓ Business Environment - Understanding of the organisation's role in the supply chain.
- ✓ Governance - Policies and procedures governing cybersecurity.
- ✓ Risk Assessment - Identification and prioritisation of risks.
- ✓ Risk Management Strategy - Processes for managing risks.

siegecyber.com.au contact@siegecyber.com.au

NIST FRAMEWORK GAP ANALYSIS

Protect (PR):

- ✓ Access Control: Policies for user access management.
- ✓ Information Protection Processes and Procedures - Security policies and standards.

Detect (DE):

- ✓ Anomalies and Events - Detection of unusual activities.
- ✓ Security Continuous Monitoring - Ongoing monitoring of systems and networks.

Respond (RS):

- ✓ Response Planning - Incident response plans.
- ✓ Communications - Coordination and communication during incidents.

Recover (RC):

- ✓ Recovery Planning - Plans for restoring systems and operations.
- ✓ Improvements - Enhancements to recovery strategies.

RECOMMENDATIONS AND ROADMAP

Provide a detailed roadmap for improving the company's cybersecurity posture:

Gap Remediation Plan:

- ✓ Specific actions to address identified gaps.
- ✓ Prioritised list of remediation steps.

Implementation Roadmap:

- ✓ Milestones and key deliverables.
- ✓ Assigned responsibilities and timelines.

Budget and Resources:

- ✓ Estimation of costs and resources required.
- ✓ Budget breakdown for remediation and implementation.

IMPLEMENTATION SUPPORT

Assist with advice on implementing recommended cybersecurity measures:

Project Management:

- ✓ Overseeing the implementation process.
- ✓ Regular status updates and progress reports.

Technical Assistance:

- ✓ Providing technical expertise and advice.

CONCLUSION

By partnering with **Siege Cyber**, you can enhance your organisation's cybersecurity maturity and ensure compliance with the **NIST Cybersecurity Framework**. Our comprehensive approach includes detailed assessments, tailored recommendations and ongoing support, providing a robust foundation for safeguarding critical assets and data.

siegecyber.com.au contact@siegecyber.com.au