



Siege Cyber offers comprehensive **SOC 2** assessments and gap analyses to help businesses 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.



SOC 2 COMPLIANCE ASSISTANCE

Identify gaps between the current security posture and the SOC 2:

Current State Review:

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

SOC 2 Mapping:

- ✓ Map existing controls to the **SOC 2 Trust Services Criteria** (Security, Availability, Processing Integrity, Confidentiality, Privacy).
- ✓ Identify gaps and areas needing improvement.
- ✓ Prioritise gaps based on risk and impact.

CYBERSECURITY SOC 2 COMPLIANCE ASSISTANCE

Conduct a detailed assessment of cybersecurity posture using the SOC 2 requirements:

- ✓ Security.
- ✓ Availability.
- ✓ Processing Integrity.
- ✓ Confidentiality.
- ✓ Privacy.



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.



CONTINUOUS MONITORING AND IMPROVEMENT

Ensure ongoing cybersecurity resilience and adherence to the SOC 2 requirements:

Regular Assessments:

- ✓ Periodic reviews and updates of the cybersecurity posture.
- ✓ Scheduled assessments to ensure continuous improvement.

Incident Response Drills:

- ✓ Simulated exercises to test and improve response capabilities.
- ✓ Tabletop exercises and live drills.

Metrics and Reporting:

- ✓ Metrics to measure the effectiveness of cybersecurity efforts.
- ✓ Regular reports to senior management.



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 **SOC 2** requirements. Our comprehensive approach includes detailed assessments, tailored recommendations and ongoing support, providing a robust foundation for safeguarding critical assets and data.