ADVISORY SERVICES

cyberSuite

cyber health assessment

Amidst an evolving cyber threat landscape and increased privacy and cyber security legislation requirements, it is more important than ever to manage your business's cyber risks. The first step to managing your risks is knowing the health of your organisation's cyber security, privacy and data protection.

WHAT IS A CYBER HEALTH ASSESSMENT?

The Cyber Health Assessment (CHA) is a risk-based cyber security, privacy, and data protection assessment built to identify your business's current cyber security standing. The assessment is tailored to the risk and business needs of SMEs and is designed to provide actionable uplift for your business. The CHA enables your business leaders to understand your organisation's security standing and provides a path to becoming more cyber resilient.

Our assessment combines multiple standards to create a holistic evaluation. These standards include:

- ACSC Essential Eight
- ISO 27001
- NIST Cybersecurity Framework
- ICO Accountability Framework
- Current Insurance Requirements
- Industry Best Practices

WHY CONDUCT A CYBER HEALTH ASSESSMENT?

Risk Reduction
The CHA is a cost-effective approach to understanding and reducing your business's cyber risks. The report and recommendation roadmap provide you with actionable steps to maximise risk reduction strategies, increase resilience, and strengthen your security posture.

Strengthened Security
You gain insights into achieving alignment with recognised standards and industry best practices for protecting your information and assets. This alignment can greatly reduce the likelihood and impact of cyber incidents affecting your business.

Expert Advice
The CHA provides your organisation with insights and advice from experts with experience in cyber security, risk management, data protection, and privacy, in addition to significant experience with the cyber insurance industry. This provides you with a holistic, expert-driven view of your cyber health.

TRAINING SERVICES

cyberSuite

cyber health assessment

OUTCOMES

Assessment Report
You will receive a report assessing your current cyber security and data protection standing. This report provides analysis of your business practices, plans, and strategy, allowing you to better understand your business's cyber maturity.

Recommendation Roadmap
You will receive a roadmap of recommendations for making improvements to your cyber controls, processes, and strategies. We categorise the recommendations by difficulty, resource requirements, and priority to help you determine where to focus your efforts first.

Confidence
Knowing your organisation's cyber health equips its leaders with the confidence they need to make informed decisions and manage risk appropriately. The CHA provides awareness of your current cyber health as well as confidence in the steps to take in improving your cyber resiliency and risk management.

SERVICE DELIVERY

Delivery Process & Timeline

Please allow 1-2 weeks for the development of deliverables from the date we receive all relevant materials.

TRAINING SERVICES

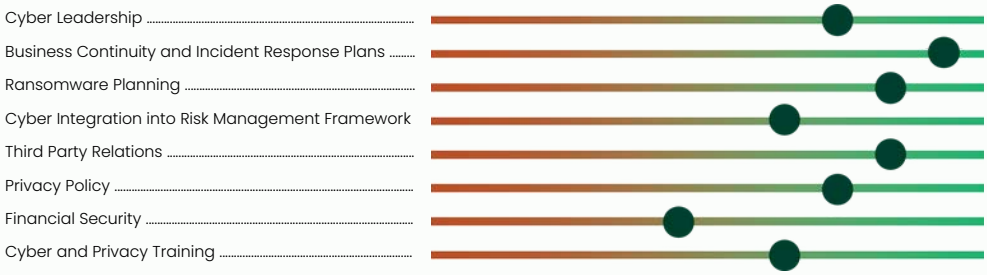
cyberSuite

cyber health assessment

EXAMPLE OF DELIVERABLES

ASSESSMENT REPORT

1. Findings and Assessment | Governance



We note the willingness of the organisation's leadership to enhance their cyber security and privacy posture. Several key areas of governance exist to develop this further. The organization should consider designating key security roles to set the organizational security culture. The current absence of Business Continuity, Incident Response (including Ransomware Planning) and Disaster Recovery Plans highlights a limited ability to maintain business continuity and respond to organisational threats. The limited processes for managing and assessing third party risks, in addition to

RECOMMENDATION ROADMAP

Priority	Implementation Difficulty	Domain	Category	Identified Risk	Recommended Action	Business Benefit	Resource Requirements
Low	Easy	Governance	Cyber Leadership	**Cyber Security Management** - No person with a dedicated job function for cyber security management which may result in a lack of expertise to identify and manage cyber threats, a lack of coordination, and lead to inadequate security	•Formally appoint a senior member of staff as the responsible person for cyber security risks and provide them with the required authority and independence to perform the role.	•Allows the organisation to have a dedicated person with the expertise to be able to identify and manage cyber threats, implement effective security measures, and liaise with multiple departments to ensure consistency in maintaining security measures and practices.	• Board Members • Executive leaders • Likely Cost: Low - None
High	Moderate	Governance	Business Continuity & Disaster Recovery	**Business Continuity** - Limited ability to manage a crisis and maintain business continuity, as well as effectively respond to an incident (Incident Response Plan).	•Develop a Business Continuity Plan for business wide impacts, not only cyber incidents. Review this policy at least annually. •Develop an Incident Response Plan (IRP) and review this policy at least annually. •Ensure the Plan includes ransomware specific response plans for appropriate preparation for a ransomware incident. •Establish a regular review schedule for the IRP and conduct at least annual tabletop exercises to test the IRP effectiveness. •Ensure that the Plans are tested and updated at least annually. •If wishing to implement, consult cyberSuite's advisory templates for guidance.	•A BCP greatly assists the business to reduce company risks in crisis situations. It ensures that business operations can continue to earn income by detailing response methods both during and after an incident. •An IRP increases the company's ability to manage a crisis by detailing business instructions for the management and mitigation actions required to effectively detect, respond to, and recover from an incident. •Make key decisions in a safe environment instead of the stressful situation of a crisis.	• Board Members • Executive leaders (CEO, CFO, COO, etc) • Department Heads • Responsible IT staff • General staff participation • Likely Cost: Low
Low	Moderate	Governance	Business Continuity & Disaster Recovery	**Disaster Recovery** – No evidence of a Disaster Recovery Plan (DRP) to assist in the recovery of disasters inflicted upon the business.	•Develop a Disaster Recovery Plan that considers natural disasters as well as human-caused disasters. •Establish a regular review schedule for the DRP and conduct at least annual tests/exercises to test the plans effectiveness. •If wishing to implement, consult cyberSuite's advisory services.	•Details the recovery procedures for reducing business interruption and methods to recover to normal operations as soon as practical, based on potential disasters inflicted upon the business.	• Executive leaders • Department Heads • Responsible IT staff • General staff participation
High	Moderate	Governance	Cyber Integration into Risk Management Framework	**Risk Management** - Enterprise level risks not being identified or mitigated, opening the risk of serious harm.	•Develop and implement an Enterprise Risk Management Framework. **OR** •At a minimum, implement a Risk Register to document the organisations business risks. •Ensure the inclusion of both cyber and privacy risks within the Framework **OR** Risk Register. •Implement an overall risk management framework using an industry leading framework	•Provides the business's leadership with direct oversight of organisational risk, not only cyber risks. •Risks can be proactively identified and pursued as they are combined with daily business activities. •Provides a greater ability to maintain legal and regulatory compliance. •Promotes increased awareness of risk while strengthening response capabilities.	• Board Members • Executive leaders & senior management • Legal, HR & Responsible IT staff • Likely Cost: Medium - Time
Medium	Easy	Governance	Supply Chain Risk	**Management of Relations with Third Parties** - No process in place to manage and assess the third parties becoming involved with [Company Name], potentially bringing unnecessary risk into the business.	•Develop and establish a process to assess third parties becoming involved with operations or more general business. •The process should primarily consist of a preventative assessment to appropriately manage and assess any risks that may be present in becoming involved with any new third parties. •Please refer to the following resources for further information. •https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/cyber-supply-chain-risk-management	•The ability to fully assess third party businesses allows them to understand the methods in which they manage and process data, while being able to evaluate potential risks to appropriately manage them and limit any repercussions which may develop.	• Executive leaders • Department Heads • External Vendor participation • Likely Cost: Low - None

Contact the cyberSuite team for more information, pricing* and bookings.

*Preferential pricing available for Emergence Insurance Policyholders.

1300 829 237

info@cybersuite.com.au

cybersuite.com.au

OUR MISSION

cyberSuite

who we are

cyberSuite is your trusted ally in navigating the intricate landscape of cybersecurity. Our team of cyber advisory specialists is dedicated to empowering individuals and businesses of all sizes. We enable you to safeguard your digital assets, offering tailored solutions to fortify your defences against evolving threats. With cyberSuite, embark on a journey of resilience, innovation, and unwavering protection in the digital age. Your cybersecurity success story begins here.

OUR TEAM

Cris White | Head of Advisory

Cris leads cyberSuite's cyber advisory team, combining his military background and risk management expertise to help organizations build resilience and navigate uncertainty. His hands-on approach spans all service areas, including conducting tabletop exercises and offering vCISO consultations.

Tai Tran | Senior Cyber Security Analyst

Tai has in-depth expertise in technology and change leadership. As an ISO27001 Lead Auditor and a holder of CISSP and CISM, Tai is passionate about assisting organisations to improve and solidify their governance and compliance practices.

Chris Lea | Cyber Security Analyst

Chris is our excited and cheerful security analyst who leads several service areas, including our Cyber Security Assessments and eDiscovery Service. He is an Associate of ISC2 and loves finding ways to improve processes and systems.

Chali Tillakaratne | Security Operations Analyst

Chali leads our Security Operations and Cyber Threat Intelligence capabilities. With a background in IT system administration, he is well versed in Microsoft platforms, as well as specialised security tooling such as Black Kite and Sentinel One.

Allana Boyd-Boland | Solicitor

Allana is a Solicitor focused on privacy and cyber law. Her expertise assists organisations by providing clarity around Privacy legislation, practical privacy policies, and providing advice for data breach eDiscovery.

OUR SERVICES

ADVISORY

- Security Assessment
- vCISO Trusted Advisor
- Supply Chain Risk
- Cyber Threat Intelligence

TRAINING

- Tabletop Exercises
- Cyber Awareness Training
- Privacy Training

SECURITY OPERATIONS

- Monitored EDR
- Vulnerability Management

INCIDENT RESPONSE

- Post Breach Remediation
- eDiscovery
- Digital Forensics

PRIVACY

- General Privacy Advice
- Privacy Training
- Data Protection