CSO GROUP Securing Australian Business

CYBER RISK & ASSURANCE

PRACTICE PROFILE

Our Cyber Risk & Assurance (CRA) service is designed to help organisations effectively manage their operational, financial, and regulatory risks while ensuring compliance with relevant laws, regulations, and industry standards. We provide a comprehensive and tailored approach to help businesses enhance their decision-making processes, safeguard assets and achieve a strong culture of compliance.

Our goal is to empower your organisation and people to navigate complex regulatory landscapes, protect valuable assets, and foster a culture of accountability and integrity. By partnering with us, you can focus on core business activities while we handle the critical aspects of risk management and compliance, ensuring your organisation's long-term success and sustainability.

www.csogroup.com.au

COMMON BUSINESS CHALLENGES IN CYBER RESILIENCY

RAPID CYBERSECURITY RISK AND THREAT LANDSCAPE CHANGES

With the ever-evolving security threat landscape, it is becoming increasingly challenging to constantly keep up-to-date with measures to protect the organisation's Crown Jewels.

LIMITED RESOURCES

Scarcity of resources (such as finances, time and people) can increase the risk that an organisation is unable to appropriately prepare for and protect from cyber threats.

STATUTORY, REGULATORY AND CONTRACTUAL OBLIGATIONS

The many statutory, regulatory and contractual obligations enforced on organisations can lead to fatigue, and therefore oversights, in the areas of compliance and manual processing.

CYBER RESILIENCE TO CYBER ATTACK

Being unprepared for a cybersecurity incident leaves the organisation exposed to increased risk and potentially unable to respond appropriately and expeditiously. This failure could lead to legal and punitive consequences and significant damage to reputation.

SUPPLY CHAIN RISK

A lapse in the monitoring of security information throughout the supply chain can open the organisation to unforeseen vulnerabilities and weaknesses. This leaves the organisation susceptible to disruptions and has the potential to significantly hinder the effective operation of the company.

CREDENTIALS OF OUR TEAM

Each member of our team has a broad risk and audit background, with extensive experience testing and designing controls. This breadth of expertise provides us with the knowledge and understanding to assist clients across a business issue, end-to-end, inclusive of business outcomes, planning, processes, people, and technology.

- ISO27001 Lead Implementer and Senior Lead Auditor
- Certified Information Security Auditor (CISSA)
- Certified Information Systems Security Professional (CISSP)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Certified Information Security Manager (CISM)
- The Open Group Architecture Framework (TOGAF)
- Sherwood Applied Business Security Architecture (SABSA)

WHY WE BUILT THIS PRACTICE

CSO Group’s CRA practice was established to facilitate and augment our clients’ security practices. We aim to support you in reducing the risk and impact from ever-evolving cyber threats to a level that is within your risk appetite.

OUR APPROACH

At CSO Group, we initiate our client engagements by collaborating with your organisation, starting from senior executive level discussions. Our aim is to provide you with a comprehensive understanding of your information security risks and assist in their effective management. By adopting a structured top-down risk-based approach, we ensure that security risks are addressed in a way that aligns with internationally recognised standards like ISO31000, ISO27001, NIST, and CIS, thus elevating your overall security posture.

Our core value lies in building a strong and trusted advisor relationship rather than simply offering solutions. Through this partnership, we work diligently to achieve business security outcomes that are tailored to meet the unique needs of your organisation, ensuring your business is well-protected and resilient in the face of potential threats.

THE RESULT

Our approach produces outcomes that enable businesses to continue doing what they do in a secure and sustainable manner.

Comprehensive Risk Management: Potential threats and vulnerabilities can be proactively managed with a professional security service that identifies, assesses, and mitigates risks effectively.

Seamless Compliance Adherence: Organisations achieve better adherence to relevant compliance regulations and industry standards, reducing the risk of penalties and legal consequences.

Efficient Governance Processes: A well-implemented information security management system (ISMS) streamlines governance structures and decision-making, leading to improved accountability and operational efficiency.

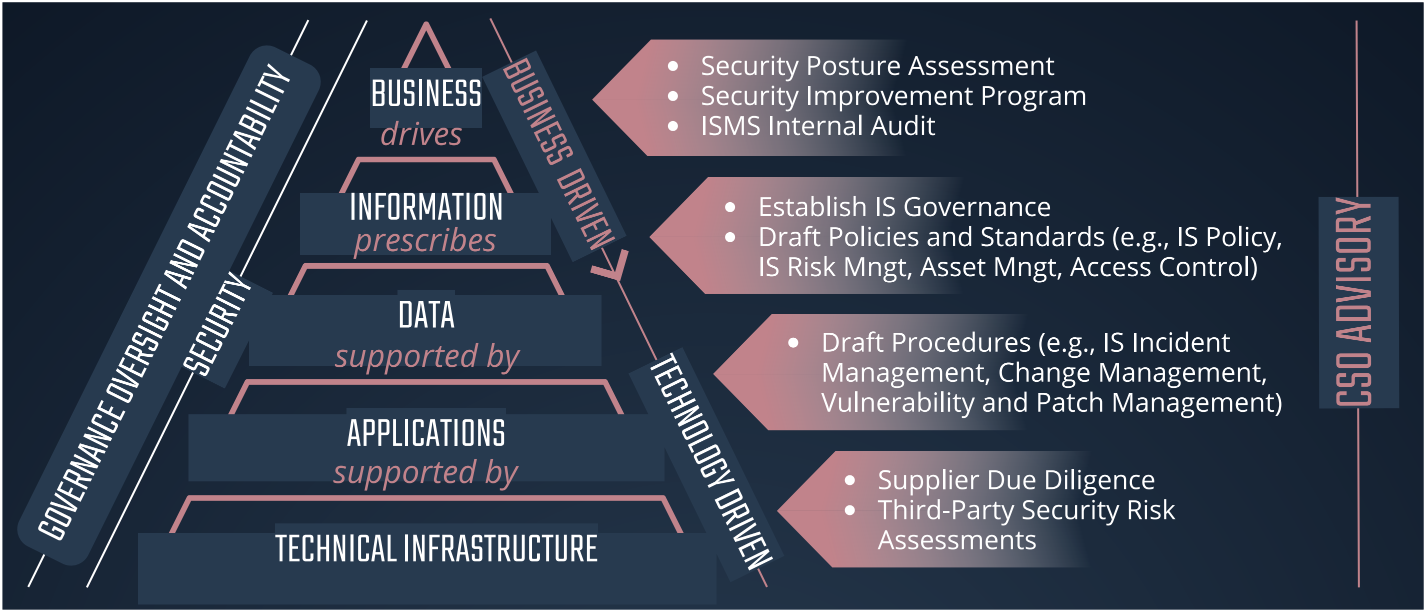
Enhanced Security Posture: The organisation's overall security posture is elevated through targeted security measures and safeguards identified by the CRA security consultants.

Stakeholder Confidence: Stakeholders gain increased confidence in the organisation's ability to protect their interests and data, fostering stronger relationships and trust.

OUR CRA PRACTICE THREE KEY SERVICES ARE:

1. Building Security Resilience
2. Supplier Due Diligence and Risk Assessment
3. ISMS Internal Audit

CSO GROUP'S CRA SERVICES



- Security Posture Assessment
- Security Improvement Program
- ISMS Internal Audit

- Establish IS Governance
- Draft Policies and Standards (e.g., IS Policy, IS Risk Mngt, Asset Mngt, Access Control)

- Draft Procedures (e.g., IS Incident Management, Change Management, Vulnerability and Patch Management)

- Supplier Due Diligence
- Third-Party Security Risk Assessments

*ENTERPRISE ARCHITECTUAL FRAMEWORK

CORE COMPETENCIES

Our competencies underpin our ability to produce business security outcomes. This is how we achieve success for our customers.

CONTEXTUAL AWARENESS

Solving business problems well requires consideration of business context. We take the time to understand business, technology, and governance aspects of a problem space. Examples include current threats, budget constraints, business goals/strategies, and resourcing.

TRUSTED ADVISORY

When we engage, we strive to establish a trusted advisor relationship at all levels, from technical through to management. Our experience has proven that this enables better collaboration, and ultimately, a better business outcome.

INDUSTRY EXPERTS

Our consultants have years of expertise in solving business problems across many industries, from government to e-commerce, education, utilities, and more. This broadens our critical thinking on possible options and factors to consider, often going beyond those considered by the organisations themselves.

NARRATION

A genuine business outcome can only be achieved when there is an end-to-end understanding of what is to be done, why it is to be done, and how it is to be done. We take our customers on the journey to understanding through storytelling. This ensures full business support, appreciation of value, and ultimately a solution that is highly consumable and successful.

1 BUILDING CYBER RESILIENCE

CREATE SECURITY BASELINE Security Posture Assessment

- The first step to managing Information Security risk is to know your current security posture. CSO Group will perform a security assessment of your environment against internationally recognised standards (e.g., ISO27001, NIST, PCI DSS) and generally accepted best practices.
- A report will then be provided that can be used to spearhead the organisation's security improvement journey.

ESTABLISH SECURITY CAPABILITIES Security Improvement Program

- CSO Group will guide you through your improvement journey to understand the context to align IS objectives to your business objectives. Following this, we will assist you in establishing ELT oversight over information security and risk.
- As part of this journey, CSO Group will facilitate the establishment of IS Policies and Standards.

ENHANCE OR AUGMENT SECURITY CAPABILITIES ISMS Operationalisation

- CSO Group will provide advisory services to assist you in operationalising the security requirements established by senior management.
- Once you have identified your Crown Jewels, CSO Group will collaborate with your key stakeholders/process owners to assess the risks and develop the risk treatment plan.
- CSO Group is also able to augment your capabilities to enhance security measures such as conducting Supplier Risk Assessments and developing IS BCM, BIA, and BCP.

MANAGED SECURITY Compliance Management

Following the enhancement of your security capabilities, CSO Group will be able to augment change to your business in the following security capabilities to enable continuous improvement:

- CISO Advisory
- ISMS Internal Audit
- IS Risk Management
- Supplier Risk Assessment
- IS BCP and DRP testing

OPTIMISE SECURITY CAPABILITIES Security-as-an-Enabler

It is important at the end of an enhancement journey to enable feedback on the effectiveness of the implemented security measures. This is achieved through the following measures, with which CSO Group can assist:

- Continuous Improvement
- Risk Treatment Plan management
- Key Performance Indicator monitoring
- KRI monitoring
- Reporting to Executive Leadership Team

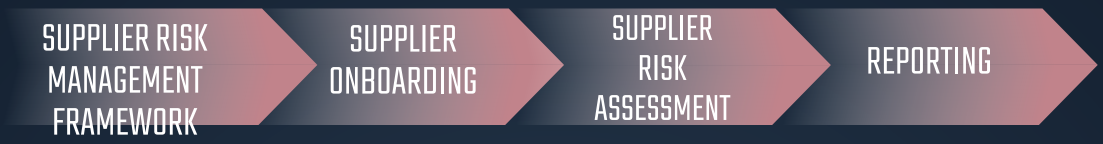
ISO27001 CERTIFICATION READY

"Building security resilience is our foundation for growth - embracing challenges, fortifying defences, and conquering the digital frontier with unwavering confidence."

*Matt Sirotich, CTO of CSO Group

2 SUPPLIER DUE DILIGENCE & RISK ASSESSMENT

CSO Group conducts Supplier Risk Assessment services on behalf of our clients. We aim to assist you in understanding your supplier risk profile, protect information outsourced, and manage compliance and contractual obligations. Leveraging a Smart Cyber Risk Management Platform, we enable our clients to gain oversight of the supply chain risk. However, if you already have a current supplier risk assessment process in place, we will be guided by that, and provide security consultants to perform the assessment.



ESTABLISH SUPPLIER RISK MANAGEMENT GOVERNANCE

CSO Group will assist you in establishing policies and standards to manage your supplier risks. To facilitate this, CSO Group will perform a walkthrough of your current practices in managing supplier risk. At the end of this initial phase, CSO Group will deliver you the drafted policies and standards for your review and approval.

PERFORM SUPPLIER RISK ASSESSMENT

Once the supplier has been onboarded, assessments can be initiated through the platform. On initiation, an email will be sent to the supplier requesting them to login and access the questionnaire. The CSO Group security consultants will collaborate with the supplier on your behalf to perform the assessment.

IDENTIFY AND ONBOARD SUPPLIERS

Following the identification of suppliers by your business process owners, CSO Group will facilitate your business in onboarding the suppliers to the platform.

DASHBOARD OVERSIGHT

Once the supplier risk assessment has been finalised, you will be able to access the platform to view the status of the supplier risk assessment performed thus far.
CSO Group will arrange a discussion with you to go over the results and next steps.

3 ESSENTIAL EIGHT IMPLEMENTATION

IDENTIFY SCOPE AND TARGETED MATURITY LEVEL

Validation of the assessment scope and confirmation that the scope and identified services are appropriately covered by the system components.
Identify a target maturity level that is suitable for the environment.

GAP ASSESSMENT AND RISK REPORTING

A gap analysis of people, process and technology control against the stipulated Essential Eight controls and strategies.

A risk-based review of the organisation's IT security processes, supporting technologies and security controls.

An assessment of the effectiveness of the controls in place to protect the organisation against common cyber security threats.

COMPLIANCE REPORT ON CURRENT MATURITY LEVEL

Conduct an audit leveraging tools and assessment processes to perform an objective measure of current cyber risk exposure and maturity level against Essential Eight strategies for the in-scope systems and applications.

RECOMMENDATION ROADMAP

Prepare a detailed roadmap from current to desired maturity level.

Create a tailored mitigation approach to effectively reduce risks and align with business objectives.

Consider additional mitigation strategies and security controls including those from the ISO 27001 Framework (ISMS) and the Australian Government Information Security Manual (ISM).

OUR PASSION IS SOLVING BUSINESS PROBLEMS

Our passion is solving business problems and genuinely helping organisations do what they do best in a secure manner with appropriately managed risk. Each member of our team shares in this view and has earned a high reputation for excellence in client delivery. We take a pragmatic approach to enabling client outcomes and building strong internal and client relationships based on trust, active engagement, and quality delivery.

Each member of our team has a broad technical background with extensive experience in advising, designing, implementing and managing various technologies. This breadth of expertise provides us with the knowledge and understanding to assist clients across a business issue, end-to-end, inclusive of business outcomes, planning, processes, people, and technology.

SAFEGUARD

Investing in our Cyber Risk & Assurance (CRA) services is a strategic imperative, as it empowers your business to confidently navigate complexities, safeguard assets, ensure regulatory adherence, and unlock a resilient future amidst evolving challenges.

CSO DELIVERY MODEL

Single Point Accountability: CSO Group act as your single point of accountability across all security technologies.

Standard Processes: Delivered through the Cyber Risk & Assurance Service, simplifying service delivery and engagement.

Shared Resources: Our cross-skilled resources share responsibility for technical and event management for thorough problem resolution.

Continuous Improvement: Our methodologies are tried and tested, with continuous improvement embedded at the core.

CSO GROUP Securing Australian Business

www.csogroup.com.au