CYBER SECURITY SOLUTIONS

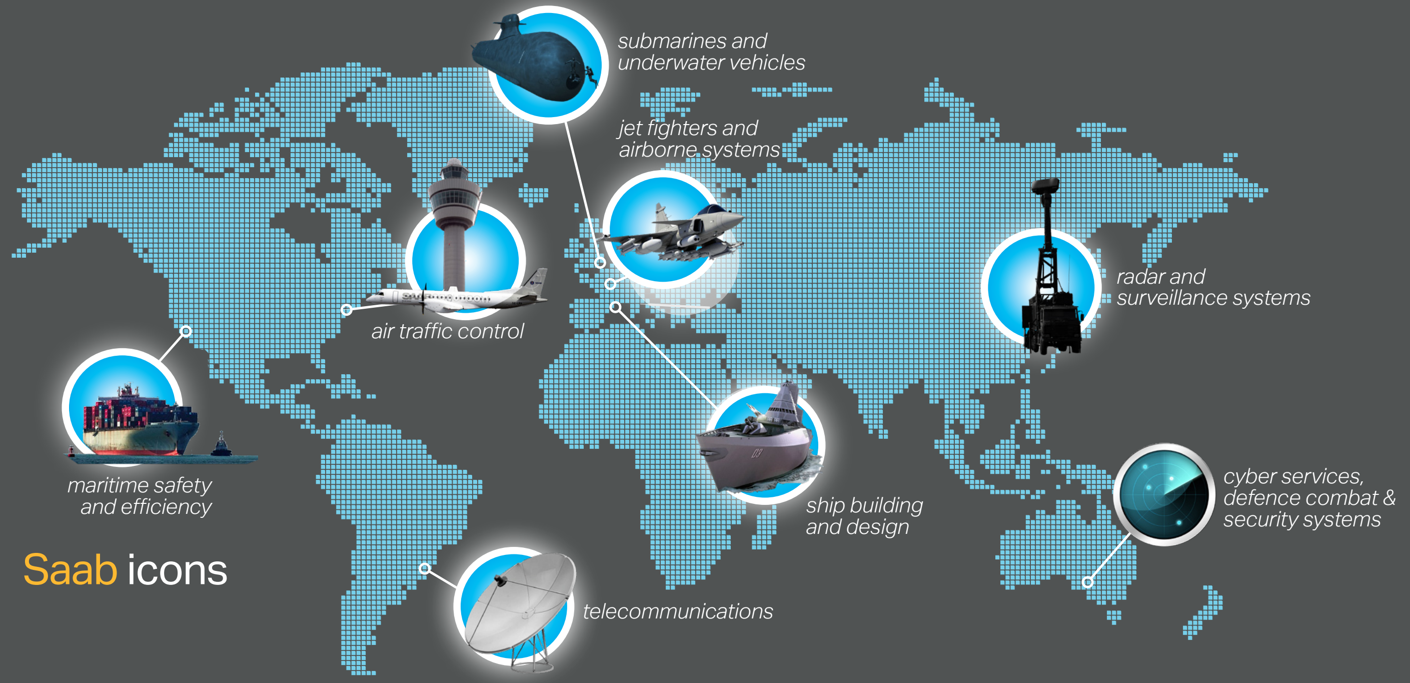
Capability Statement

Keeping people, society and information **safe**

Saab's led defence, aviation and security technology for more than eighty years.

As government, business and military reliance on information, networks, and communication technology has increased significantly over the past decade, so to has the frequency of advanced, sophisticated cyber attacks.

As a trusted, world-leader of defence and security technology, we've got the 'thinking edge' on leading the fight to combat the cyber threat.


submarines and underwater vehicles
jet fighters and airborne systems
air traffic control
radar and surveillance systems
maritime safety and efficiency
ship building and design
cyber services, defence combat & security systems
telecommunications

Saab icons

Our story

Saab is a high-technology, defence and security business-to-government and business-to-business organisation with 17,000 employees worldwide.

No other technology company designs and builds submarines, aircraft, underwater vehicles, missiles, torpedoes, radars, camouflage, security systems, plus everything in-between, to **keep people and society safe**.

Our **information and cyber security risk management consultancy** is built on Saab's primary values —trust, expertise and drive. Always ahead of technology. A reputation for integrity. Committed to our core philosophy of safety ... we're passionate about **keeping information and systems safe.**

Capability and capacity

Saab Australia's information and cyber security capability was built upon the need to protect our own intellectual property and systems, as well as that of our clients. As an organisation developing military and civil systems to defend our national interests and safeguard our critical infrastructure and public safety, protecting that information is absolutely critical. To demonstrate our ongoing commitment to our own information and cyber security, Saab was one of the first defence companies in Australia to achieve **ISO 27001 certification** for its information security management system.

As well as protecting our own systems, we build resilience into the products and systems we develop for our customers. We make sure our products and systems are 'cyber hardened' to withstand the demanding threat environments in which they operate.

Over many years we built our in-house experience to support Saab's systems worldwide and build a professional security and risk consulting business which offers a comprehensive suite of information and cyber security services.

We have selected our information and cyber security team through careful design - securing the best professionals with the highest level of experience and knowledge. Our consultants are skilled communicators, who can lead your information and cyber security project from inception through to completion, giving you complete continuity.

Our security risk advisors, assessors, analysts and information technology specialists have the highest government and defence security clearances and are trusted and respected by federal, state and local governments nation-wide. Our experience spans the defence, government, communications, utilities, health, education, law, finance and hospitality sectors.

Our information and cyber security offer

The framework and systems protecting Saab's information assets are independently audited and certified to the internationally recognised ISO/IEC 27001:2013 standard. We follow these same principles in our information and cyber security consulting work.

Cyber security strategy

We will work with your organisation to develop your information and cyber security strategy, aligned with your organisational and security objectives.

IRAP assessments & preparedness

An IRAP assessment is the first stage towards achieving accreditation to process, store or communicate government or nationally sensitive information. Our IRAP program is led by our IRAP assessors who are certified by the Australian Signals Directorate (ASD). We can also assist your organisation prepare for an IRAP assessment or accreditation, by advising on and implementing appropriate security standards, requirements, controls, and recommendations in accordance with the Australian Government ISM.

Governance, risk and compliance

We will review your organisation's controls, policies and procedures to determine your level of information and cyber security maturity and ability to manage risk. These activities typically align to industry standards and frameworks such as ISO 27001, ISM, PSPF/DSPF, CPS 234, CMMC and NIST.

Product cyber resilience engineering

Whether implementing a new system or upgrading existing or legacy systems, we will work with you to develop or enhance your organisations cyber resilience. By employing a systems security engineering approach we provide the necessary guidance to navigate cyber resiliency to ensure deployed products or systems survive confronting threats.

DISP preparedness

We will work with you to enhance your information and cyber security maturity in order to meet or exceed the Defence Industry Security Program (DISP) requirements at all levels (Entry through to Level 3). Across all four membership categories of Governance, Physical and Personnel Security as well as Information and Cyber Security.

Penetration testing

We perform objective-based penetration tests to identify vulnerabilities in your organisation's infrastructure, services and applications. Tests can be conducted as an anonymous user seeking to exploit weaknesses in the systems and services visible on the internet or as an internal user attempting to elevate privileges or exfiltrate data.

Security architecture

We will determine whether the controls within a network/communications environment are effective and appropriate for your current business requirements and threat profile, aligned with vendor and industry best practice; and recommend a course of action.

System configuration and security reviews

These reviews assess your server and IT system configurations against industry and vendor best practices; typically covering security configuration, password strength testing, software maintenance, firewalls, and network infrastructure—tailored to your needs.

Incident response

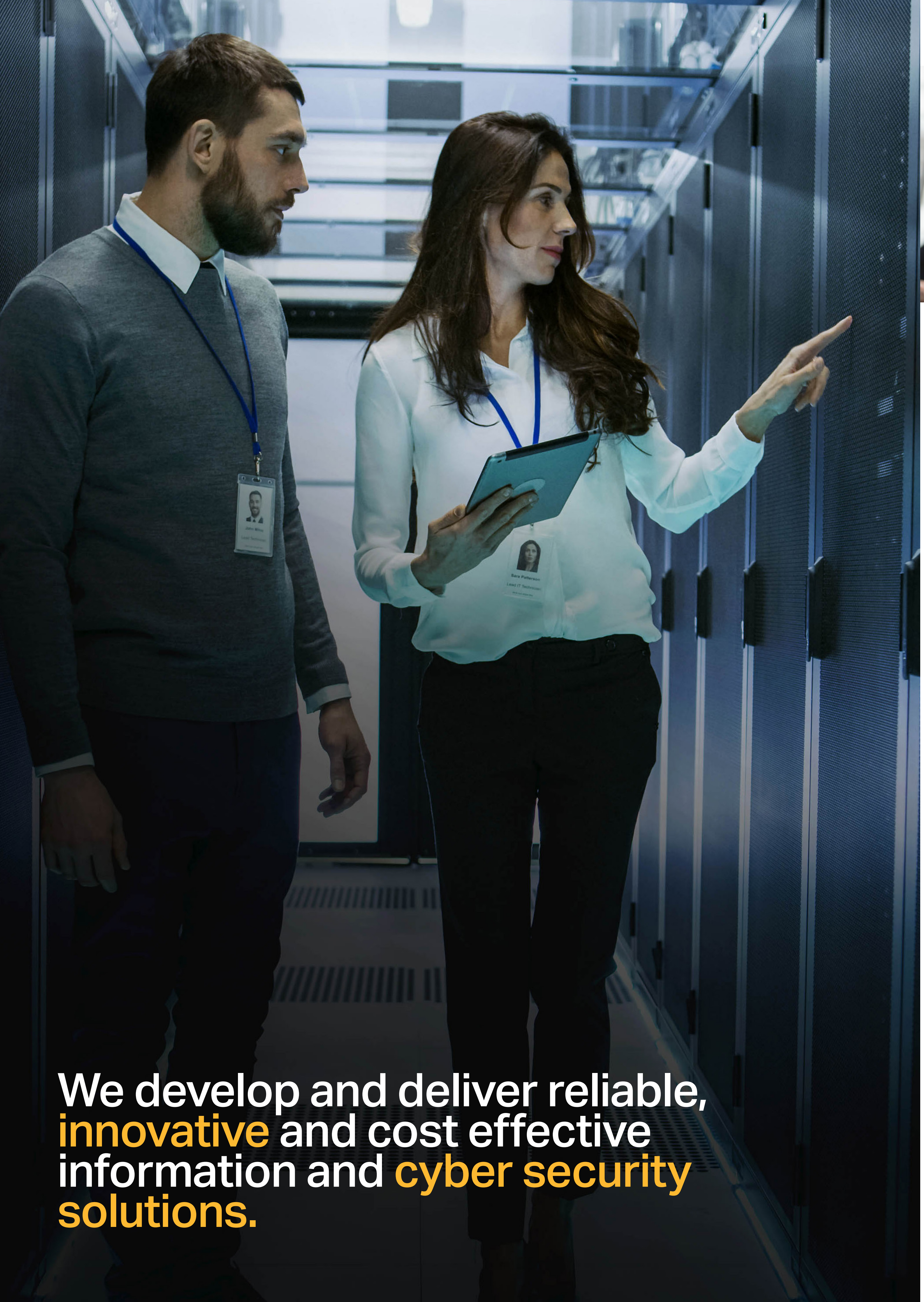
Our on-demand service supports you by providing assistance with incident handling and related discovery activities following a cyber-related breach or significant event.

Training and awareness

We develop and deliver tailored security awareness programs relevant to your workforce. Most security breaches are a result of human error or social engineering. It can be something as innocent as clicking a link, or downloading a malicious file. We'll also help you create policies and procedures to establish a clear framework for developing your information and cyber security culture and governance. We can provide either technical or practical education, training and awareness packages to suit individuals' or organisations' responsibilities.

Supply chain risk management

Managing the supply chain is an important piece of an organisations approach to risk management. Knowing where and how the supply chain interacts with your organisation is critical in ensuring business continuity for your organisation and implementing security best practice. We will work with you to develop or enhance your knowledge of your systems and understanding of your supply chain to identify the inherent risks that arise throughout the supply chain process and help you develop appropriate mitigation strategies to effectively manage your supply chain risk.



We develop and deliver reliable, innovative and cost effective information and cyber security solutions.

OUR CLIENTS

Education institutions (public & private)
Defence & defence industry
Financial bodies
Federal & state government agencies
Electronics & technology/automation production industries
Saab Group and its defence & security customers

Work snapshots

For the most part, a lot of the work we do is focussed on building resilience for our clients in order to protect them from the ever evolving information and cyber security threats. We act with integrity and confidentiality to protect the privacy of every client.

CASE STUDY

Not for profit organisation

As well as its own operational data, this organisation stored the personal information of its workforce and its tens of thousands of donors, supporters and members. Saab performed a series of internal and external penetration tests of their network to determine how safely the systems were managing this data. We detected a critical vulnerability, which if left untreated, could have made all of the personal identity information they stored to be breached, causing enormous reputational damage and ultimately threatening the ongoing viability of their organisation. Saab provided the appropriate advice and guidance for the organisation to mitigate this risk.

CASE STUDY

Business email compromise

We helped a small to medium enterprise interrupt the theft of almost $1,000,000 through the compromise of their email system. When the company discovered the problem and engaged Saab to manage their incident response, we were able to quickly construct an attack timeline and capture and catalogue email and computer accounts involved in the incident. Tracing the initial phishing email that lead to multiple account compromises revealed the steps the attackers took to inject themselves into the client's email chain and coerce them into sending money to a fraudulent bank account. Using this information we established mitigation strategies to prevent further compromise and developed an education program for the business to maintain. Saab was able to provide valuable information to the client which was then used by the authorities to further their investigation, ultimately identify the perpetrators and disrupt the BEC operation.

CASE STUDY

National defence organisation

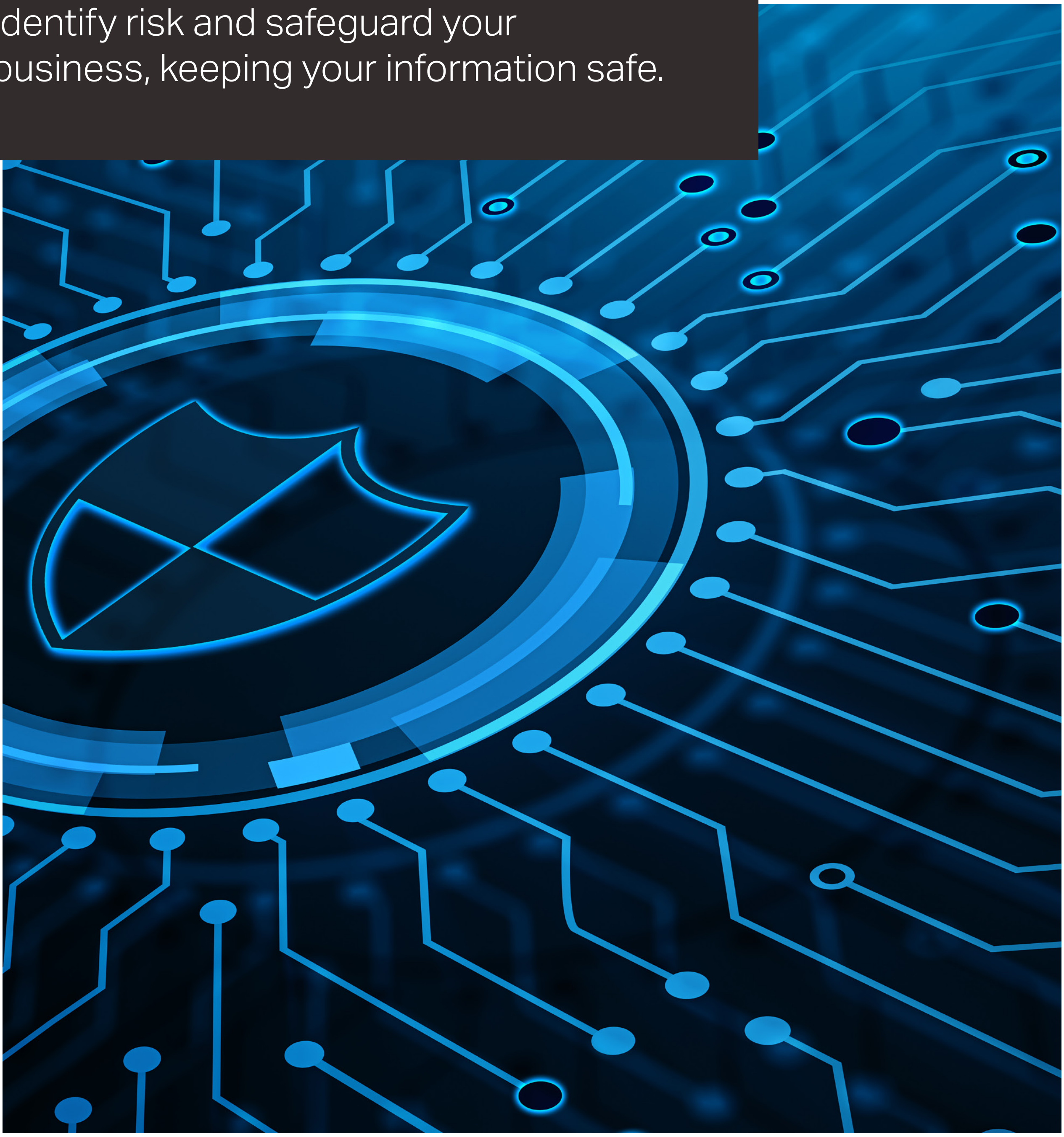
Keeping our national defence agencies' data safe is a critical element of maintaining our nation's security. Saab reviewed the organisation's information management systems and structure to create a new management framework to meet Information Security Registered Assessors Program accreditation. Saab developed system overview documents, system security plans, incident response plans, security risk management plans, statements of applicability and a suite of policies and procedures.

CASE STUDY

Saab Australia

Saab has been a trusted supplier of advanced military and civil security system for more than thirty years. The relentless trend of managing and sharing information online has exposed Saab and its business partners' systems to possible information theft or disruption. To further enhance our own information and cyber security posture we implemented our own information security management system obtaining ISO/IEC 27001 certification for our Australian operations. A complete framework with structured plans, national cyber security policies, procedures, work instructions and an ongoing employee awareness scheme was developed, initiated and is now in rolling review. Saab is now adopting the model globally for international security management and accreditation.

Identify risk and safeguard your business, keeping your information safe.



Saab Australia Pty Ltd
21 Third Avenue, Mawson Lakes, South Australia 5095

Contact us: SaabAU.Cyber@au.saabgroup.com