Answerspecific®

CAPABILITY STATEMENT

Information Security Consulting

Our Story

Launched in 2018, Answerspecific's team of cybersecurity professionals specialises in risk-based cybersecurity management, designing organisation-specific roadmaps for cybersecurity governance, compliance and risk management. We not only build your Information Security Management System (ISMS) from ground up but also help it to align with frameworks and regulations including ISO/IEC 27001, AICPA SOC2, NIST CSF, APRA CPS234, EU GDPR, CCPA. We have qualified cybersecurity professionals with a wealth of experience in this space. Our experience extends across government, start-ups, consulting firms, financial and health sectors.

Why your business needs us

Cybersecurity has a dynamic landscape and the emergence of new processes, technologies and regulations dictate that businesses implement new strategies to mitigate evolving security risks and meet compliance challenges.

The team at Answerspecific is committed to optimising cybersecurity and risk management practices. We are passionate about keeping people, systems and information safe in the cyberspace.

Our capabilities

Our core areas of expertise are end-to-end information security management system (ISMS) implementation, cybersecurity risk management, compliance reviews to various security frameworks, standards & privacy regulations*, cybersecurity assessments, cybersecurity & control audits.

Based in Perth, Western Australia, our Cybersecurity Governance Risk and Compliance (GRC) services facilitate compliance to frameworks such as IEC/ISO 27001, SOC 2 (AICPA), CPS234 (APRA), Cybersecurity Framework (NIST CSF) and privacy regulations such as GDPR (EU) and CCPA (California).

Our clients

Our diverse client base includes those in government, start-ups, consulting firms, financial and health sectors located in Australia and the United States.

* We are not legal advisers or legal counsel, our advice for regulatory compliance is general in nature.

Our Services & Our Approach

We build ISMS (Information Security Management System) from the ground up

Every organisation is inherently different due to the domain it operates in, the technologies used, the market, the operational jurisdiction, its internal culture, the governing legislation, etc.

Building a successful and continually improving ISMS requires all of these key factors to be considered. At AnswerSpecific, we understand that this requires a cultural change within the organisation which needs to be initiated by the top management. Hence, we work with the higher management, and many times with the board & the CEO to create and implement a holistic ISMS.

We help build a risk awareness culture

Cybersecurity is best managed by building risk culture within the organisation. This approach also helps the Board and the Senior Management understand threats to the organisation and ultimately help them decide on the right strategies to mitigate those risks. These strategies progressively pervade all levels of the organisation to create a robust risk-aware culture. We adopt a holistic approach in which we take into account the organisation's vision, mission, current practices and stakeholder interest to formulate an organisation-specific framework to fortify its cybersecurity landscape.

For organisations with an ISMS already in place

We conduct risk & gap assessment including cybersecurity audits. We utilise industry accepted auditing principles such as ISO 19001 to perform these reviews so that the review/audit results paint a precise reflection of the organisation's current state.

We review your organisation's controls, policies and procedures and perform staff and manager interviews to determine the level of information and cybersecurity maturity and ability to manage risk. These reviews typically align to industry standards and frameworks such as ISO/IEC 27001, NIST CSF, SOC 2, etc. We then utilise the outcome of such assessments to close gaps by working with relevant teams thereby raising organisation's cybersecurity maturity level and resilience.

Other Services

Security architecture & system configuration reviews

Our team will determine whether the controls within your business network and communications environment are suitable and effective. These assessments typically cover security configuration, server configurations, firewalls, network infrastructure. Controls should align with vendor and industry best practice recommendations. If not, we will recommend optimal changes to strengthen any weak controls.

Application reviews

Utilising secure system engineering principles, our team delivers guidance to ensure deployed products or systems survive confronting threats. Whether implementing a new system, upgrading existing or legacy systems, we will work with your business to refine or reinforce your cyber resilience.

Supply chain risk management

Our team will work with you to identify risks that arise throughout the supply chain and identify the weak links. Our team will then help you to map out appropriate mitigation strategies to effectively manage your supply chain risk. Managing the supply chain is an important part of your organisation's approach to risk management. Understanding where and how the supply chain interacts with your organisation is key to implementing security best practices.

Ethical hacking & penetration testing

With our dedicated pen testing partners, we identify, test and highlight vulnerabilities in your networks, applications, external websites or internal systems.

SaaS application security reviews

If you are a SaaS provider, our team works with you to assess your application, policies, procedures and application development practices to meet customer security requirements and to help you achieve certifications such as SOC 2 or ISO 27001, certifications that your customers have been asking in their security screening questionnaires.

Regulations (thinking of expanding into the EU?)

Our team will help you align with EU GDPR so that your business is compliant at the outset of your EU activities. We have developed an easy and effective approach to help your organisation achieve and maintain its obligations to this EU Privacy Law.

Cybersecurity frameworks that we implement include

- ISO/IEC 27001
- EU GDPR
- SOC 2 (AICPA)
- NIST CSF
- CPS234 (APRA)
- Information Security Manual (ISM)
- Protective Security Policy Framework (PSPF)

Additional Services Offered

CISO-as-a-Service (CISOaaS) / Virtual CISO (vCISO)

Security Manager as a Service (SMaaS)

Work Snapshots

User Case 1

IT Vision (a Perth based supplier of Payroll, and other applications to local government and councils): our team helped IT Vision to implement ISMS from the ground up and helped them achieve ISO 27001 certification. They received their certification in December 2021.

User Case 2

We helped an Australian Datacentre achieve ISO 27001 certification.

User Case 3

Our team started working with a SaaS application provider based in the United States to help with SOC 2 reports, ISO 27001 certification, GDPR & CCPA alignment. They are now GDPR and CCPA compliant and have received their SOC 2 Type 1 report. They are on their way to achieve a favourable SOC 2 Type 2 report and ISO 27001 certification.

Address

Level 17, 2 The Esplanade,
Perth WA 6000, Australia

Tel / Mob

T: +61 8 6146 1327
M: +61 417 567 567

Email

contact@answerspecific.com.au

www.answerspecific.com.au