Privasec GRC
GOVERNANCE AND INFORMATION SECURITY PARTNERS

ISO 27001 (ISMS) CERTIFICATION
Fact Sheet v2.2

The rapid growth in cyberattacks is changing market expectations. Shareholders, customers, and partners expect a higher level of security than ever before to protect their businesses and information. Companies have traditionally invested in a range of security controls and technologies to protect themselves, but with no real end to end strategy, and little returns. Without tangible returns for the business, many CISOs, CIOs, and Security Officers see their security funds reduced to bare OpEx minimums.

ISO27001:2013 allows companies to use world class risk management standards to strategise and coordinate their security investments whilst getting marketable recognition for it. Many businesses, including Government Departments, are now insisting that their suppliers and contractors demonstrate that they have a secure environment as a mandatory requirement for doing business.

Privasec has a proven track record in establishing and operating non-shelf ware Information Security Management Systems (ISMSs) certified to ISO27001.

Top 10 Reasons to achieve ISO27001 Certification

1. Minimise the business reputational/financial and legal impact in the event of a security breach.
2. Comply with a contractual requirement.
3. Access larger/bigger clients/tender like multinational and government agencies.
4. Win a tender/contract renewal.
5. Gain a competitive edge/stay competitive (depending on the industry).

For CISO/CIO/Security Officers to:

6. Show tangible value to the business though the marketable certification stamp.
7. Link ad-hoc existing security controls together and improve ROI through a strategic and consistent approach to security.
8. Spread risks to the business where they belong.
9. 'Lock in' annual security funding year after year (talk to us to find out how).
10. Stop wasting time answering the same ISO-based security questionnaires in tenders.

HOW THIS SERVICE WORKS

Privasec will establish an ISMS compliant with ISO27001 for you to operate and train your staff accordingly. All our ISMSs are tailored to the organisation needs, governance mechanism and maturity levels. In larger organisations, existing security and risk management frameworks are often leveraged to deliver a more integrated ISMS offering.

The ISMS establishment process follows the known Plan-Do-Check-Act (PDCA) cycle prescribed by ISO27001. As part of the PDCA cycle Privasec will assess your security risk and work with you to create an associated risk treatment plan. The risk treatment plan will constitute a security roadmap for security officers, who can rely on the identified risks to create compelling business cases and secure funding.

Speak to your consultant to get a detailed understanding of the Plan-Do-Check-Act ISMS cycle. Your consultant will also walk you through our baseline ISMS project plan and methodology.

WHAT YOU GET

Business Executives

- Recognised certification.
- Maturity and Security Assurance to market & shareholders.

Sales Teams

- Ability to demonstrate security credentials, get invited to, and win more tenders.

CIOs/CISO/Security Officers

- Tangible and visible benefits delivered to the business/executives (via the certification).
- Visibility, understanding and most importantly, ownership of security risks by the executives.
- A "lock in" annual flow of risk-based security investment.
- A trusted advisor who knows your business intimately and is only a phone call away.

Security Teams

- More visibility from the business. Access to create strong business cases.
- Significant time saving responding to security questionnaire in tenders.
- Translated IT security problems into tangible business impact.

NEXT STEPS

Privasec has years of experience in implementing ISMS and achieving certification for its clients. Your consultant will be happy to discuss the details of your ISMS implementation plan and how to best leverage your company's existing strength.

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia

ISO 27001 (ISMS)
Frequently Asked Questions v2.0

What is the relation between ISO27001 and ISMS?

ISMS stands for "Information Security Management System" which is the title of the ISO27001 standard. ISO27001 is made of a set of clauses to provide guidance on the creation or a best practice ISMS system to manage security risks and drive improvements in a company's security posture.

In annexure A of ISO 27001 a list of common security controls (Security Policy framework, HR security, physical security, network security, etc.) are listed and is used to effectively assess all aspects of an organisation.

ISO27001 Annexure controls Vs. ISO27001 clauses

Security Officers commonly mistake annexure controls with the ISO27001 standard clauses, thus thinking that certification is near impossible for their companies. The ISO27001 certification recognises the ability for an organisation to manage their security risks and certification is not dependant on all annexure controls being implemented and matured.

"We struggle to get funding for basic security tools/Our security posture is shocking. ISO27001:2013 is a distant dream."

In our experience, ISMSs are an invaluable tool to secure a repeatable flow of risk based security investment from the business. Since ISO27001 requires security risks to be formally owned by business/ executives the sole accountability for security is moved out of the IT department and shared with business.

Will the project impact on my current operations?

Privasec has a very hands on approach and will built the entire ISMS for you. Limited but regular input will however be required from the management team. The risk assessment process is a one-time impact on operational staff and requires between 30-120 minutes of their time depending on their specific role.

Can Privasec certify me? What is the difference between Privasec and SAI Global?

SAI Global, BSI or Loyds are certification bodies. They conduct the final certification audits and therefore cannot consult and help you with the establishment of your ISMS.

Privasec is not a certification body and therefore cannot certify organisations. Your Privasec consultant will however act on your behalf at the audit and guide the primary auditee during the certification audit.

Will you mitigate my risks for me? Isn't that a conflict of interest?

Privasec is an independent firm, not a technology integrator and does not partner with any vendors. Privasec does not mitigate risk on behalf of clients. Our aim is to assist our client's through the remediation process and advise on suitable options and technologies where required. We may be able to, at the request of customer, carry out work if it falls within our service offering.

Privasec GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS RED RED TEAMING & ADVANCED ETHICAL HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia