ISO 27001 :2022

ISO/IEC 27001:2022

Information Security Management System Certification

Certified 2023 - Valid Through 2026

QuantSec Pty Ltd

Australian Cybersecurity Solutions Provider

ABN: [Company ABN]

Website: www.quantsec.com.au

Email: compliance@quantsec.com.au

Overview

This document certifies that QuantSec Pty Ltd has successfully implemented and maintains an Information Security Management System (ISMS) that complies with the requirements of ISO/IEC 27001:2022, the international standard for information security management systems.

Certification Body: [Certification Authority Name]

Certificate Number: ISO27001-QSEC-2023-[Number]

Initial Certification Date: [Date]

Current Certificate Valid Until: [Date]

Next Surveillance Audit: [Date]

What is ISO/IEC 27001:2022?

ISO/IEC 27001:2022 is the latest version of the internationally recognized standard for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The standard provides a systematic approach to managing sensitive company information, ensuring it remains secure through people, processes, and technology controls.

Key Components of Our ISMS

- **Rigorous Information Security Management:** Comprehensive policies and procedures covering all aspects of information security
- **Risk Assessment and Mitigation:** Systematic identification and treatment of information security risks
- **Continuous Improvement Processes:** Regular reviews and updates to security controls and procedures
- **Annual Third-Party Audits:** Independent verification of our ISMS effectiveness and compliance

ISO 27001:2022 Standard Structure

The ISO 27001:2022 standard is organized into the following clauses, all of which QuantSec maintains compliance with:

Clause	Section	Description
Clause 4	Context of the Organization	Understanding organizational context, needs, and scope of the ISMS
Clause 5	Leadership	Management commitment, policy, and organizational roles
Clause 6	Planning	Risk assessment, risk treatment, and security objectives
Clause 7	Support	Resources, competence, awareness, communication, and documentation
Clause 8	Operation	Operational planning, risk assessment, and risk treatment
Clause 9	Performance Evaluation	Monitoring, measurement, analysis, and internal audit
Clause 10	Improvement	Nonconformity, corrective action, and continual improvement

Section 1: Context of the Organization

QuantSec has thoroughly documented the internal and external issues relevant to our ISMS, including the interested parties and their requirements. This ensures our security management system is aligned with our business objectives and stakeholder expectations.

Example: Internal and External Issues

Company Context: QuantSec, as a cybersecurity solutions provider, develops and delivers information security services for businesses across Australia.

External Issues:

- Regulatory: Compliance with Australian Privacy Principles (APP), GDPR, and industry-specific regulations

- Market: Growing customer demand for ISO 27001 certification from third-party providers
- Threat Environment: Increasing sophistication of ransomware attacks and cyber threats targeting Australian infrastructure

Internal Issues:

- Growth: Rapid scaling of development and engineering teams requires robust security oversight
- Culture: Company culture emphasizes rapid feature development while maintaining security best practices
- Resources: Commitment to ongoing security training and awareness for all personnel

ISMS Scope

Our ISMS covers all aspects of our business operations, including:

- Information technology infrastructure and systems
- Client data processing and storage
- Internal business operations and communications
- Third-party vendor and supplier relationships
- Physical security of office and data center facilities
- Personnel security and access management

Section 2: ISMS Support Documentation

In accordance with Clause 7 of ISO 27001:2022, QuantSec maintains comprehensive support documentation including:

2.1 Resources

- Dedicated Information Security Team with qualified security professionals
- Chief Information Security Officer (CISO) reporting to executive management
- Security operations center (SOC) for 24/7 monitoring
- Investment in security tools, technologies, and infrastructure

2.2 Competence and Awareness

- Regular security awareness training for all employees (quarterly)
- Role-specific security training for technical staff
- Phishing simulation exercises and incident response drills
- Professional certifications including CISSP, CEH, and security-specific qualifications

2.3 Communication

- Internal communication protocols for security incidents and updates
- External communication procedures for client notifications
- Security bulletin distribution and awareness campaigns
- Regular security committee meetings and reporting

2.4 Documented Information

- Information Security Policy (reviewed annually)
- Risk Assessment and Treatment Plans
- Statement of Applicability (SoA)
- Security procedures and work instructions
- Incident response playbooks

- Business continuity and disaster recovery plans

Section 3: ISMS Operation

QuantSec's ISMS operation (Clause 8) encompasses systematic processes for identifying, assessing, and treating information security risks across all areas of our business.

3.1 Operational Planning and Control

- Documented procedures for all critical security processes
- Change management controls for system modifications
- Secure software development lifecycle (SDLC) practices
- Configuration management and baseline controls

3.2 Information Security Risk Assessment

We conduct comprehensive risk assessments on a regular basis (at minimum annually, and when significant changes occur):

- Asset identification and classification
- Threat and vulnerability analysis
- Impact and likelihood assessment
- Risk evaluation and prioritization

3.3 Information Security Risk Treatment

Based on our risk assessments, we implement appropriate controls selected from:

- ISO 27001:2022 Annex A controls (93 security controls across 4 themes)
- Additional controls specific to our business requirements
- Industry best practices and regulatory requirements

Section 4: Performance and Improvement

4.1 Monitoring and Measurement (Clause 9)

QuantSec maintains a comprehensive performance evaluation program:

- **Continuous Monitoring:** Real-time security event monitoring and log analysis
- **Security Metrics:** Key performance indicators (KPIs) tracked monthly
- **Internal Audits:** Conducted quarterly by independent internal auditors
- **Management Review:** Executive review of ISMS performance quarterly

4.2 Internal Audit Program

Our internal audit program ensures ongoing compliance and effectiveness:

- Planned audits covering all areas of the ISMS annually
- Audit findings tracked and resolved within defined timeframes
- Audit reports reviewed by management
- Follow-up audits to verify corrective actions

4.3 Continual Improvement (Clause 10)

We are committed to continual improvement of our ISMS effectiveness through:

- Analysis of nonconformities and root causes
- Implementation of corrective and preventive actions
- Lessons learned from security incidents
- Regular updates to security controls based on emerging threats
- Feedback from internal audits and management reviews

> **Improvement Initiative Examples:**
>
> - Enhanced multi-factor authentication deployment across all systems
> - Implementation of zero-trust network architecture principles
> - Upgraded security information and event management (SIEM) platform

- Expanded security awareness training program with gamification

Annex A Controls Implementation

ISO 27001:2022 Annex A contains 93 information security controls organized into 4 themes. QuantSec has conducted a thorough assessment of all controls and implemented those applicable to our operations as documented in our Statement of Applicability (SoA).

The Four Annex A Themes:

- **Organizational Controls (37 controls):** Policies, governance, human resources, asset management
- **People Controls (8 controls):** Personnel security, awareness training, disciplinary processes
- **Physical Controls (14 controls):** Physical site security, equipment protection, environmental controls
- **Technological Controls (34 controls):** Access control, cryptography, network security, incident management

Sample Implemented Controls

- **A.5.1 Information Security Policy:** Board-approved policy reviewed annually
- **A.5.7 Threat Intelligence:** Subscriptions to threat feeds and participation in security forums
- **A.6.1 Screening:** Background checks for all employees with access to sensitive information
- **A.8.1 User Endpoint Devices:** MDM solution managing all company devices
- **A.8.2 Privileged Access Rights:** Least privilege principle enforced with regular reviews
- **A.8.10 Information Deletion:** Secure deletion procedures for all media types

Audit and Certification Process

QuantSec underwent a rigorous two-stage audit process to achieve ISO 27001:2022 certification:

Stage 1: Documentation Review

- Review of ISMS documentation and readiness
- Assessment of information security policy and objectives
- Evaluation of risk assessment methodology
- Review of Statement of Applicability

Stage 2: Implementation Audit

- On-site assessment of control implementation
- Interviews with management and staff
- Technical security testing and verification
- Review of records and evidence
- Assessment of ISMS effectiveness

Ongoing Surveillance

To maintain certification, QuantSec undergoes:

- Annual surveillance audits by the certification body
- Recertification audit every three years
- Continuous monitoring and improvement between audits

Benefits to Our Clients

QuantSec's ISO 27001:2022 certification demonstrates our commitment to information security and provides our clients with:

- **Assurance:** Independent verification of our security practices
- **Confidence:** Demonstrated commitment to protecting client data

- **Compliance:** Support for clients' own regulatory and compliance requirements
- **Risk Reduction:** Systematic approach to identifying and mitigating security risks
- **Best Practices:** Alignment with international standards and industry best practices
- **Continuous Improvement:** Ongoing enhancement of security controls and processes

Contact Information

For questions about our ISO 27001:2022 certification or to request additional documentation, please contact:

> **Compliance & Governance Team**
>
> Email: compliance@quantsec.com.au
>
> Phone: +61 (0)2 1234 5678
>
> Business Hours: Monday - Friday, 9:00 AM - 5:00 PM AEST

QuantSec Pty Ltd | ABN: [Company ABN]

ISO/IEC 27001:2022 Certified Information Security Management System

This document is provided for informational purposes. For the official certificate and Statement of Applicability, please contact our Compliance Team.

Document Version: 1.0 | Last Updated: November 2025

© 2025 QuantSec Pty Ltd. All rights reserved.