# CASE STUDY – ISO27001 Governance Success

## Client Background

Our client is a rapidly growing satellite R&D organisation developing next-generation space technologies for commercial, defence, and government applications.

As the organisation expanded internationally, security expectations from customers, investors, and strategic partners increased significantly. The leadership team recognised that existing processes, developed during the start-up phase, would not adequately support continued growth, complex supply chains, and increasing cyber risk obligations.

At a critical growth stage, the organisation engaged our security consulting practice to strengthen governance and achieve ISO/IEC 27001:2022 certification.

## The Challenge

Like many technology scale-ups, growth had outpaced governance maturity.

Key challenges included:

### Governance Gaps

- Limited visibility of enterprise information assets
- Inconsistent ownership of security responsibilities
- Informal risk management processes
- Limited executive reporting on cyber risk

### Operational Challenges

- Rapid onboarding of staff and contractors
- Growing supplier ecosystem
- Increasing volumes of sensitive R&D data
- Multiple cloud platforms and business systems

### Customer Requirements

- Many prospective customers required evidence of:
- Mature information security management
- Risk management practices
- Supplier assurance capabilities
- Independent certification
- Without recognised certification, competitive opportunities were increasingly difficult to secure.

## Our Approach

We adopted a pragmatic business-first methodology designed specifically for high-growth technology companies.

## Phase 1: Governance Assessment

## We performed a comprehensive review covering:

- Organisational governance
- Information security practices
- Existing controls
- Risk management maturity
- ISO 27001:2022 readiness

## Deliverables included:

- Gap Assessment Report
- Executive Risk Summary
- ISMS Roadmap
- Prioritised Remediation Plan

## Phase 2: Governance Framework Design

Working with executive leadership, we established a governance structure aligned with organisational objectives.

Key improvements included:

*Security Governance Committee*

Established clear oversight responsibilities across:

- Executive Team
- Engineering Leadership
- Technology Teams
- Business Operations

## Risk Management Framework

Implemented:

- Enterprise risk registers
- Risk ownership model
- Treatment planning
- Regular governance reporting

## Policy Framework

Developed and aligned policies covering:

- Information Security
- Access Management
- Supplier Security
- Incident Management
- Asset Management
- Cryptography
- Business Continuity

## Phase 3: ISO 27001:2022 ISMS Implementation

Our consultants designed and embedded a sustainable Information Security Management System (ISMS).

Key activities included:

- Scope definition
- Asset identification
- Risk assessments
- Statement of Applicability development
- Control implementation
- Metrics and performance reporting
- Internal audit capability development

The objective was not simply certification, but a security program capable of scaling alongside the business.

## Phase 4: Change Management & Security Culture

Technology controls alone do not create a secure organisation.

We therefore focused heavily on:

- Security awareness training
- Executive engagement workshops
- Process ownership
- Governance reporting
- Continuous improvement practices

This ensured long-term adoption rather than a compliance-only exercise.

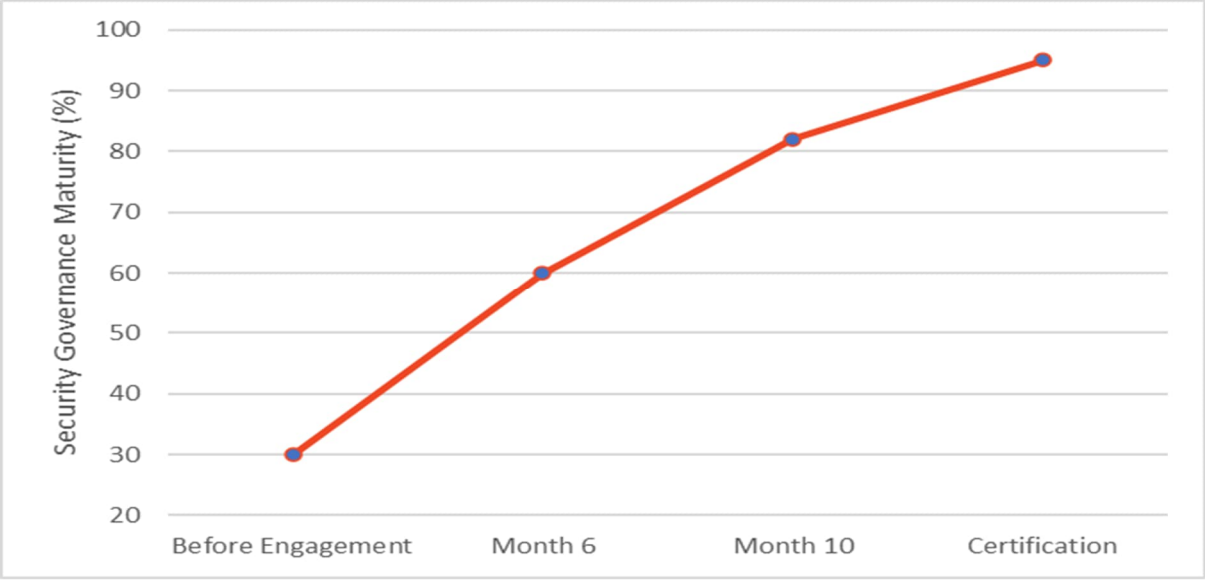
## Phase 5: Certification Readiness

Prior to the external audit we conducted:

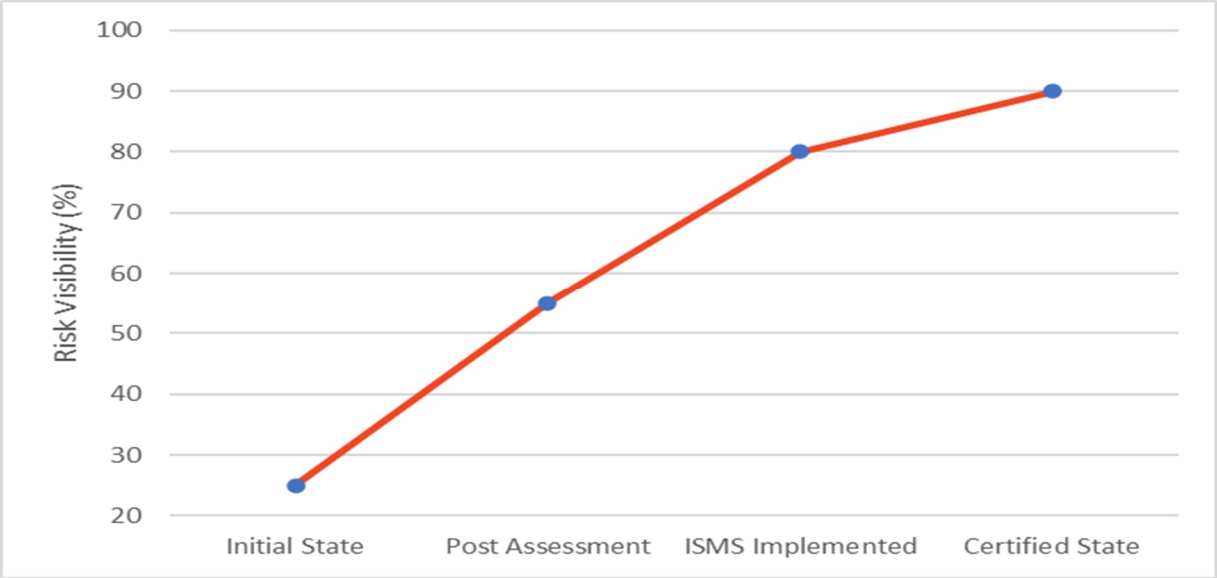
- Internal audits
- Management reviews
- Evidence validation
- Control effectiveness testing
- Audit simulations

By the time the certification auditor arrived, the organisation had confidence in both its controls and governance processes.

## Results and Outcomes




## Information Risk Visibility



## High-Level Outcomes

| Metric | Improvement |
|---|---|
| **ISO 27001:2022 Certification** | Achieved |
| **Information Risk Visibility** | +70% |
| **High-Risk Findings** | -60% |
| **Policy Coverage** | +90% |
| **Audit Readiness** | +85% |
| **Governance Reporting** | Fully Implemented |

## Business Impact

The benefits extended well beyond certification.

Improved Customer Confidence

ISO 27001 certification became a valuable trust signal during commercial engagements and procurement processes.

## Executive Visibility

Leadership gained improved insight into:

- Security performance
- Emerging risks
- Compliance obligations
- Third-party risk exposure

## Scalable Governance

The governance model now supports:

- International growth
- New technology platforms
- Increased staff numbers
- Future compliance initiatives

Enhanced Security Culture

Security became embedded as a business responsibility rather than solely an IT concern.

## Client Testimonial

“The consulting team provided a clear roadmap, practical guidance and executive-level expertise that allowed us to mature our governance framework while maintaining focus on innovation. Achieving ISO 27001:2022 was a significant milestone that strengthened customer confidence and positioned us for continued growth.”

**— Head of Information Security, Satellite Technology Organisation**

## Why Organisations Choose Us

We specialise in helping growing technology organisations achieve meaningful security outcomes—not simply compliance.

Our consultants combine expertise across:

- ISO/IEC 27001:2022
- Security Governance
- Risk Management
- GRC Programs
- MSSP Services
- Security Operations
- Cloud Security
- Internal Audit & Assurance

We understand the challenges faced by scaling organisations and build security programs designed to support growth rather than slow it down.

## Ready to Strengthen Your Governance and Achieve ISO 27001:2022?

Whether your organisation is preparing for certification, responding to customer requirements, or seeking to mature security governance, our team can help.

### Our Services

- ISO 27001 Readiness Assessments
- ISMS Design & Implementation
- Governance Uplift Programs
- Risk Management Frameworks
- Internal Audits
- Virtual CISO (vCISO)
- Managed Security Services

### Contact Us

📞 1800 234 357

✉️ elevate@quogroup.com.au

🌐 www.quogroup.com.au

**Build trust. Reduce risk. Scale securely.**