WOOLLEMIA INFOSEC

Case Study

ISO/IEC 27001 Readiness & Certification Support for a Growing IT Services Provider

Industry	Information Technology Services
Engagement Type	ISO/IEC 27001:2022 Readiness Assessment & Certification Support
Scope	Information Security Management System (ISMS) covering corporate IT, cloud infrastructure, and client service delivery operations
Standards Referenced	ISO/IEC 27001:2022, ISO/IEC 27002:2022, Annex A Controls
Core Services Delivered	Gap Assessment, Risk Assessment & Treatment, ISMS Documentation Support, Control Implementation Guidance, Internal Audit Preparation, Management Review Support

Executive Summary

As organizations increasingly depend on formal information security certifications to win enterprise contracts, satisfy regulatory expectations, and reassure customers, ISO/IEC 27001 has become a baseline requirement across many industries. Achieving certification requires far more than documentation; it requires a functioning, risk-based Information Security Management System embedded into daily operations.

A growing IT services provider engaged Woollemia Infosec to guide its organization through ISO/IEC 27001:2022 readiness, from initial gap assessment through to internal audit preparation, ahead of its formal certification audit. The organization needed an experienced partner to translate the standard's requirements into practical controls suited to its size and operating model.

Woollemia Infosec conducted a structured gap assessment against ISO/IEC 27001:2022 and its Annex A controls, supported the client in building a risk assessment and treatment methodology, guided the development of required ISMS documentation, and helped implement missing technical and organizational controls.

The engagement enabled the client to build a sustainable, audit-ready ISMS, strengthen its overall security governance, and approach its certification audit with confidence.

Client Overview

The client is a growing IT services provider delivering managed infrastructure, cloud, and application support services to customers across multiple industries. As its customer base expanded to include regulated and enterprise clients, the organization faced increasing pressure to formally demonstrate its information security governance through independent certification.

The organization operates a mix of internal corporate systems, cloud-hosted infrastructure, and client-facing service delivery platforms, supported by a growing internal team spanning engineering, operations, and client support functions.

Prior to this engagement, the organization had a number of informal security practices in place but lacked a documented, risk-based management system aligned with a recognized international standard.

Business Challenge

The client needed to achieve ISO/IEC 27001 certification within a defined timeline to satisfy contractual requirements from several enterprise customers, but had limited internal experience with the standard's requirements, documentation expectations, and audit process.

Existing security practices were inconsistently documented, risk assessments were informal or absent, and there was no clearly defined Statement of Applicability identifying which Annex A controls applied to the organization's operations and why.

The organization also needed to ensure that new controls could be practically adopted by its teams without significantly disrupting day-to-day service delivery, and that the resulting ISMS would remain sustainable and auditable well beyond the initial certification date.

Our Understanding

Woollemia Infosec recognized that ISO/IEC 27001 readiness is not a one-time documentation exercise, but the establishment of an ongoing risk management discipline that must be embedded into how an organization actually operates.

Our team understood that a growing IT services provider needed controls that were proportionate to its size and risk profile, rather than an overly complex framework borrowed from much larger enterprises. We focused on building a pragmatic, right-sized ISMS that satisfied the standard's requirements while remaining genuinely usable by the client's teams.

Our Solution

Initial Gap Assessment

Woollemia Infosec conducted a structured gap assessment comparing the client's existing policies, technical controls, and operational practices against the requirements of ISO/IEC 27001:2022 and its Annex A control set, producing a prioritized list of gaps to address.

Risk Assessment and Treatment Methodology

Our consultants worked with the client to define a formal risk assessment methodology, facilitating workshops to identify information security risks across people, process, and technology, and guiding the development of a risk treatment plan aligned with the organization's risk appetite.

Statement of Applicability Development

Our team supported the client in evaluating each Annex A control for applicability, documenting justification for inclusion or exclusion, and mapping each applicable control to existing or planned implementation evidence.

ISMS Documentation Support

Woollemia Infosec guided the development of core ISMS documentation, including the information security policy, scope statement, risk assessment records, asset inventory, access control policy, incident management procedures, and supplier security requirements.

Control Implementation Guidance

Our consultants provided practical guidance for implementing missing technical and organizational controls identified during the gap assessment, including access management practices, logging and monitoring, secure configuration baselines, and third-party risk management processes.

Employee Awareness and Training Support

Recognizing that a management system depends on people as much as documentation, our team supported the client in developing security awareness content and training materials to help staff understand their responsibilities under the new ISMS.

Internal Audit Preparation

Ahead of the client's certification audit, Woollemia Infosec conducted an internal audit simulation, reviewing evidence, interviewing process owners, and identifying any remaining nonconformities so the organization could address them proactively.

Management Review Support

Our consultants helped the client prepare for its first formal management review, structuring the agenda and supporting evidence required to demonstrate leadership oversight of the ISMS, a core requirement of the standard.

Business Value Delivered

The engagement gave the client a functioning, audit-ready Information Security Management System aligned with ISO/IEC 27001:2022, built around risk rather than static checklists.

The organization approached its certification audit with well-organized documentation, clearly justified control decisions, and internal teams who understood their roles within the ISMS, significantly reducing audit risk and last-minute remediation pressure.

Beyond certification, the client gained a sustainable governance framework that supports ongoing risk management, strengthens customer trust, and provides a foundation for future compliance requirements as the business continues to grow.

Why Woollemia Infosec

Woollemia Infosec supports organizations through the full ISO/IEC 27001 journey, from initial gap assessment through certification audit and beyond, combining deep knowledge of the standard with practical, business-aware implementation experience.

Rather than delivering generic templates, we work closely with client teams to build a management system that fits their actual operating environment, risk profile, and growth trajectory.

Conclusion

This representative engagement demonstrates Woollemia Infosec's ability to guide organizations through ISO/IEC 27001 readiness in a practical, business-aligned manner.

By supporting gap assessment, risk management, documentation, control implementation, and audit preparation, we helped the client build a sustainable ISMS and approach certification with confidence, strengthening its ability to compete for security-conscious enterprise customers.