SEVEN STEP
CONSULTING
ENABLING TRUST!

CASE STUDY

INDUSTRY: CYBER SECURITY AND NETWORK SERVICES PROVIDER

COMPLIANCE FRAMEWORK: ISO/IEC 27001:2022 (ISMS)

COPYRIGHT AND DISCLAIMER

.

CASE STUDY CYBER SECURITY AND NETWORK SERVICES PROVIDER ISO/IEC 27001:2022 (ISMS) IMPLEMENTATION TO STRENGTHEN SECURITY GOVERNANCE AND CUSTOMER ASSURANCE FOR A CYBER SECURITY SERVICES PROVIDER

Note: This case study is prepared for marketing/portfolio use. Operational details are presented in ranges and generalized language to avoid disclosure of confidential information.

Engagement Snapshot	
Primary service	ISO/IEC 27001:2022 (ISMS)
Industry focus	Cyber Security Products & Network Services
Delivery model	Seven Step Framework (Define to Drive) + evidence-led audit readiness
Website	https://www.sevenstepconsulting.com/

CLIENT OVERVIEW

Field	Details
Client	Cyber security and network services provider (client anonymized) Managed detection and response, network security operations
Industry	Cyber Security Products & Network Services
Company size (range)	Approx. 120-450 employees
Geography	India with customers across multiple states

INDIA WITH CUSTOMERS ACROSS MULTIPLE REGIONS

BUSINESS CONTEXT

The organization delivered security-critical services for enterprise customers and needed a formal ISMS to demonstrate consistent security governance, risk management, and evidence of control operation. ISO/IEC 27001:2022 was chosen to strengthen customer assurance and standardize internal security practices.
Trigger points included:

- Enterprise customers requested ISO 27001 evidence during onboarding and renewals.
- Service expansion increased the need for consistent governance over access, monitoring, incident handling, and vendor dependencies.
- Security audits and due diligence required repeatable documentation and evidence packs.
- Leadership sought measurable security outcomes tied to operational performance.

CHALLENGES

- Evidence needed standardization across multiple service lines and operational tools.
- Risk management required consistent scoring, ownership, and treatment tracking.
- Access controls and privileged actions needed periodic review and traceable approvals.
- Supplier risk (tools, partners, subcontractors) required formal assessment and oversight.
- Incident and problem handling needed structured post-incident reviews and improvement actions.

ENGAGEMENT OBJECTIVES

- Implement an ISO/IEC 27001:2022-aligned ISMS with governance, policies, and control ownership.
- Complete risk assessment and risk treatment planning with measurable closure tracking.
- Establish an evidence-led audit readiness program for certification and customer reviews.
- Improve customer trust and sales enablement through standardized security assurance artefacts.

SEVEN STEP CONSULTING APPROACH

Phase	What we did
Define	Confirm ISMS scope, service boundaries, and critical assets; establish governance and responsibilities.
Discover	Run ISO 27001 gap assessment and evidence discovery across operations, engineering, HR, and leadership.
Design	Create ISMS blueprint, risk methodology, SoA mapping, and prioritized control implementation roadmap.
Document	Develop policy suite, SOPs, registers, and audit artefact templates for consistent evidence capture.
Deploy	Operationalize controls for access, incident management, supplier assurance, logging/monitoring, and change governance.
Do & Check	Conduct training, internal audits, CAPA closure, and certification audit readiness checks.
Drive	Set continuous monitoring cadence with management reviews, metrics reporting, and improvement tracking.

- ISMS scope, policy, governance model, and roles/responsibilities.
- Risk register, risk treatment plan, and Statement of Applicability (SoA).
- Evidence repository structure and control-wise evidence checklists.
- Internal audit plan and reports; CAPA tracker and corrective action evidence.
- Management review pack and minutes template; KPI dashboard definitions.
- Awareness training and role-based training for control owners and operations teams.
- Customer assurance pack for onboarding and security questionnaires.

OUTCOMES AND BUSINESS IMPACT

- Improved enterprise assurance through an audit-ready ISMS and standardized evidence packs.
- Better risk visibility and treatment tracking through owned risk registers and governance cadence.
- Improved operational security through disciplined access reviews, supplier oversight, and incident handling.
- Reduced audit effort by organizing evidence and artefacts in a consistent structure.
- Sustainable compliance posture through continuous monitoring and management review rhythm.

STANDARDS AND FRAMEWORKS COVERED

- ISO/IEC 27001:2022 - Information Security Management System (ISMS).
- ISO/IEC 27002:2022 - Control guidance reference.
- SOC 2 mapping considerations (where customer contracts demand additional assurance).

SEVEN STEP
CONSULTING
ENABLING TRUST!

Seven Step Consulting Pvt. Ltd.

+91 8115609560

info@sevenstepconsulting.com

www.sevenstepconsulting.com

1006, 10th Floor, EMAAR Capital Tower 1, MG Road Sikanderpur, Sector 26, Gurugram, Haryana – 122002 (INDIA)