CyberSapiens
THE CYBER SECURITY EXPERTS

BLUEPOLARIS

Case Study

ISO 27001 CASE STUDY

Case Study

From fragmented security to certified ISMS

Customer : Blue Polaris

Industry : Consultancy

Services : ISO 27001

Blue Polaris

A global AI, analytics, and decision management consultancy — resolved 99% of identified risks and built a resilient, audit-ready information security program in one implementation cycle.

99%	6	100%
Risks resolved or mitigated	Critical security gaps closed	Org-wide policy coverage achieved

THE CHALLENGE

SECURITY FRAGMENTED ACROSS EVERY LAYER

Blue Polaris is a global AI, analytics, and decision management consultancy — and the evolution of Decision Management Solutions, a trusted IBM Premier Gold Business Partner with over a decade of experience. As the business scaled its digital footprint and distributed workforce, it had no unified information security framework. Critical gaps emerged across remote access, endpoints, and access management, creating compounding risk that demanded urgent attention.

Unsecured remote work

WFH environments lacked secure access controls, increasing exposure of sensitive client data

Weak access controls

Shared and batch passwords across teams, with no enforced password policies or role-based access.

Department silos

Varying risk levels across teams with no structured ownership or accountability framework.

Endpoint & USB blind spots

No USB control, no MDM, and no centralized endpoint visibility — leaving data leakage unchecked.

Fragmented antivirus

Non-standardized antivirus deployments with no centralized monitoring or threat visibility.

Low security culture

Limited employee awareness of cyber risks, phishing threats, and compliance obligations.

THE SOLUTION

A structured, risk-driven ISMS implementation

We designed and implemented an ISO 27001-aligned Information Security Management System for Blue Polaris, spanning governance, technical controls, and people — across the entire organization.

1

Organization-wide risk assessment

Comprehensive department-level risk identification, risk register creation, and treatment planning with clear ownership assigned at every level.

2

ISO 27001-aligned policy framework

Designed and enforced access control, password, and remote work policies standardized across all departments and roles.

3

Technical controls & endpoint hardening

USB ports restricted, advanced antivirus deployed centrally, and endpoint security strengthened across all devices.

4

Access management overhaul

Eliminated shared credentials, implemented strong password policies, and introduced role-based access controls (RBAC) org-wide.

5

Secured remote work model

Established compliant WFH infrastructure with a defined MDM strategy and clear remote access policies.

5

Security awareness & training

Delivered organization-wide training covering phishing, compliance obligations, and data handling responsibilities.

RESULTS

Measurable impact across the entire organization

“The implementation transformed our security posture — from fragmented practices to a structured, audit-ready framework that clients and stakeholders can trust.”

99% of risks resolved

Nearly all identified vulnerabilities were addressed through policy, technical controls, or structured treatment plans.

Stronger data security

Endpoint protection, USB controls, and access management eliminated major data leakage vectors.

Compliant remote work

A secure and auditable WFH model now supports a distributed global workforce without compromising data integrity.

Audit-ready foundation

Governance, monitoring, and policy standardization create a scalable base for future audits and growth.

Enhanced client trust

Demonstrated compliance readiness strengthens credibility with enterprise clients and partners.

Security culture shift

Employees now understand their role in protecting information, with accountability embedded at every level.

CyberSapiens

CyberSapiens unites our country's most trusted experts in delivering an unparallel, comprehensive end-to-end portfolio of complex and challenging threat environment. complex and challenging threat environment. cyber security services across Australia and India , Canada, USA.

Contact us to find out how CyberSapiens can boost the cyber security skills of your entire organization.

www. cybersapiens.com 1300 507 668 sales@cybersapiens.co

CyberSapiens
THE CYBER SECURITY EXPERTS