TERMINUS SYSTEMS | Speak Business. Think Security.

SECURITY POSTURE ASSESSMENT WORKSHOP

Know Where You Stand. Understand What Matters. Decide What Comes Next.

A practical, evidence-based workshop designed to help organizations understand their current information security posture, identify where improvement is needed, quantify potential loss, determine implementation urgency, and establish a clear foundation for the next stage of security improvement or an ISMS initiative.

WHAT YOU WILL DO

1 ASSESS YOUR CURRENT SECURITY POSTURE

Evaluate your organization at an executive level across 26 information security domains, identifying strengths, weaknesses, and areas requiring improvement.

Output: Current Security Status Report.

2 QUANTIFY POTENTIAL LOSS

Use your business sector, revenue, information assets, and record characteristics to estimate the potential impact of inadequate security, including ransomware and data-breach scenarios.

Outputs: Loss Estimation Report, Ransomware & Data Breach Loss Estimation Report, Loss Estimation Dashboard, Benchmarking Report.

3 DETERMINE IMPLEMENTATION URGENCY

Evaluate how urgently security improvement is required based on industry, users, compliance obligations, customer and business requirements, corporate data, technology complexity, incidents, and other organizational factors.

Output: Implementation Urgency Level Report.

4 DEFINE THE PROJECT & ITS BOUNDARY

Translate assessment findings into a clear implementation direction by defining the necessity, objectives, scope, and optimal boundary across business units, products and services, locations, and information assets.

Outputs: Implementation Necessity & Goals Report, Optimal Boundary Definition.

5 ANALYZE PRIORITY SECURITY DOMAINS

Conduct a deeper assessment of the security domains identified as requiring significant improvement, using relevant technical and organizational information.

Outputs: Domain Security Posture Analysis Report, Overall Analysis Diagram.

6 EVALUATE ORGANIZATIONAL READINESS

Determine whether the organization is prepared to undertake security improvement or an ISMS initiative by assessing information availability, culture and maturity, processes, objectives and strategy, management, and organizational structure.

Output: Readiness Assessment Report.

WHO SHOULD ATTEND?

- CISOs and information security leaders
- CEOs and business executives involved in security decisions
- IT and security managers
- Risk, compliance, and audit professionals
- ISMS project leaders
- Security governance and GRC professionals
- Managers responsible for improving organizational security posture

WHAT YOU WILL TAKE AWAY

By the end of the workshop, you will have a structured understanding of:

- Where your organization currently stands across key security domains
- What security areas require greater attention
- What potential losses may result from inadequate security
- How urgent security improvement may be
- What an appropriate implementation boundary looks like
- Which domains require deeper assessment
- Whether the organization is ready to proceed
- What information is needed to establish a structured security improvement initiative

THE ASSESSMENT JOURNEY

Assess → Quantify → Prioritize → Define → Analyze → Evaluate Readiness

Participants work through the assessment methodology using structured assessment forms and practical organizational information rather than discussing security posture only at a theoretical level.

THE ASSESSMENT FOUNDATION

The workshop applies a risk-based, business-aligned approach supported by principles including due care/due diligence and cost–benefit optimization, with reference to:

ISO/IEC 27001 | ISO/IEC 27005 | NIST CSF
COBIT | NIST SP 800-30 | ISO/IEC 27002

FROM SECURITY UNCERTAINTY TO EVIDENCE-BASED DECISIONS

Current Posture → Potential Loss → Urgency → Scope → Domain Analysis → Organizational Readiness

Security becomes easier to improve when you first understand where you stand.