

Cybersecurity Risk Assessment

Overview

The Cybersecurity Risk Assessment service provides organizations with a structured approach to identifying, evaluating, and managing cybersecurity risks. Through the development of a comprehensive risk register, organizations gain clarity on their risk landscape and the effectiveness of their control environment. Available in three tiers - Express, Standard, and Enterprise - this service is scaled to meet the unique needs of organizations at different stages of growth and complexity.

Value of Engagement

Express Tier (Small Business Focus):

- **Rapid Risk Identification** | Quick identification of critical risks affecting core business operations
- **Cost-Effective Analysis** | Focused assessment delivering maximum value within budget constraints
- **Essential Controls Mapping** | Clear linkage between top risks and fundamental security controls
- **Actionable Recommendations** | Practical, prioritized guidance suitable for smaller organizations
- **Foundation Building** | Establishment of basic risk management practices for future growth

Standard Tier (Mid-Market Focus):

- **Comprehensive Coverage** | Broader risk assessment across multiple departments and functions
- **Industry-Specific Insights** | Analysis tailored to sector-specific threats and compliance requirements
- **Detailed Control Assessment** | In-depth evaluation of control effectiveness and gaps
- **Risk Trending Analysis** | Identification of patterns and emerging risks within the organization
- **Benchmark Comparison** | Industry-specific risk comparison and best practice alignment

Enterprise Tier (Large Organization Focus):

- **Strategic Risk Management** | Integration of cybersecurity risks with enterprise risk framework
- **Complex Environment Analysis** | Assessment across multiple business units and locations
- **Advanced Risk Modeling** | Sophisticated analysis of risk interconnections and cascading impacts
- **Custom Framework Development** | Tailored risk assessment methodology for unique organizational needs
- **Executive-Level Insights** | Strategic recommendations aligned with business objectives

Scope of Assessment

Express Tier:

- 2-3 key departments
- Up to 5 stakeholder interviews
- Focus on top 15-20 critical risks
- Core security controls assessment
- Basic risk register development

Standard Tier:

- Multiple departments
- Up to 10-12 stakeholder interviews
- Comprehensive departmental risk assessment
- Detailed control environment analysis
- Industry-specific risk considerations

Enterprise Tier:

- Multiple business units/locations
- 15+ stakeholder interviews
- Deep dive into operational, strategic, and emerging risks
- Complex control ecosystem evaluation
- Custom assessment framework development

Methodology

Our tiered approach includes:

Express Tier:

- **Rapid Risk Discovery** | Focused workshops with key stakeholders
- **Standard Template Application** | Efficient risk documentation using proven frameworks
- **Critical Control Mapping** | Essential security control assessment
- **Priority Risk Analysis** | Evaluation of highest impact threats
- **Basic Mitigation Planning** | Fundamental risk treatment recommendations

Standard Tier:

- **Comprehensive Workshops** | Extended stakeholder engagement sessions
- **Industry Framework Alignment** | Sector-specific risk assessment methodology
- **Detailed Control Analysis** | In-depth security measure evaluation
- **Risk Pattern Analysis** | Identification of risk trends and relationships
- **Robust Mitigation Strategies** | Detailed risk treatment planning

Enterprise Tier:

- **Strategic Planning Sessions** | Executive-level risk workshops
- **Custom Framework Development** | Organization-specific assessment methodology
- **Advanced Control Evaluation** | Complex control ecosystem analysis
- **Sophisticated Risk Modeling** | Detailed impact and probability assessment
- **Comprehensive Treatment Planning** | Strategic risk management recommendations

Deliverables



Express Tier:

- Focused Risk Register
- Critical Risk Summary
- Basic Control Gap Analysis
- Priority Recommendations
- Executive Summary



Standard Tier:

- Comprehensive Risk Register
- Detailed Control Assessment
- Industry Benchmark Comparison
- Detailed Recommendations
- Implementation Roadmap
- Risk Trending Analysis



Enterprise Tier:

- Advanced Risk Model
- Strategic Risk Analysis
- Custom Assessment Framework
- Complex Control Ecosystem Map
- Executive Dashboard
- Strategic Recommendations
- Detailed Implementation Program
- Risk Management Playbook

Our Cybersecurity Risk Assessment service provides organizations with clear visibility into their risk landscape and practical guidance for risk management. Each tier is designed to deliver maximum value based on organizational size, complexity, and maturity, ensuring that organizations receive appropriate depth of analysis and actionable recommendations aligned with their needs and resources.