Risk Assessment Methodology

Risk Assessment Overview

Systematic process to identify, analyze, and evaluate information security risks.

Conducted annually and when significant changes occur. Informs security strategy and resource allocation.

Risk Identification

Identify threats: Cyberattacks, insider threats, natural disasters, system failures, human error.

Identify vulnerabilities: Unpatched systems, weak configurations, inadequate controls, process gaps.

Identify assets: Data, systems, applications, infrastructure, people.

Threat Analysis

Analyze threat sources: External attackers, insiders, competitors, nation-states, hacktivists.

Assess threat capabilities and motivations. Consider threat intelligence and industry trends.

Evaluate likelihood of threat exploitation.

Vulnerability Assessment

Technical vulnerability scanning of systems and applications. Configuration reviews against security baselines.

Penetration testing to identify exploitable vulnerabilities. Process and control reviews.

Assess vulnerability severity and exploitability.

Asset Valuation

Determine asset value based on: Confidentiality, integrity, availability requirements.

Consider: Business impact of loss, regulatory requirements, replacement cost, reputation impact.

Classify assets by criticality to operations.

Risk Analysis

Combine threat likelihood and vulnerability severity. Assess potential impact to confidentiality, integrity, availability.

Calculate risk level: Risk = Likelihood × Impact.

Consider existing controls and their effectiveness.

Risk Evaluation

Compare calculated risks against risk appetite. Prioritize risks for treatment.

High risks require immediate attention. Medium risks addressed in planned timeframe. Low risks may be accepted.

Risk Treatment Options

Mitigate: Implement controls to reduce risk. Accept: Acknowledge risk and accept consequences (for low risks).

Transfer: Use insurance or outsourcing to transfer risk. Avoid: Eliminate activity causing risk.

Document risk treatment decisions and rationale.

Control Selection

Select controls based on: Risk level, cost-effectiveness, feasibility, regulatory requirements.

Consider: Technical controls (firewalls, encryption), administrative controls (policies, training), physical controls (locks, cameras).

Implement defense in depth with multiple control layers.

Risk Treatment Plan

Document planned risk treatments with: Responsible party, timeline, resources required, success criteria.

Track implementation progress. Verify control effectiveness after implementation.

Residual Risk Assessment

Assess remaining risk after controls implemented. Determine if residual risk is acceptable.

Additional controls may be needed if residual risk too high. Document accepted residual risks.

Risk Monitoring

Continuously monitor risk landscape. Track new threats and vulnerabilities.

Monitor control effectiveness. Conduct periodic risk reassessments.

Update risk register with changes.

Risk Reporting

Report risk assessment results to management and board. Highlight: Top risks, risk trends, treatment progress.

Provide risk-based recommendations for security investments.

Quarterly risk updates to leadership.

Risk Register

Maintain centralized risk register documenting: Identified risks, risk ratings, treatment plans, owners, status.

Risk register is living document updated regularly. Used for risk tracking and reporting.

Compliance Integration

Integrate compliance requirements into risk assessment. Ensure controls address regulatory obligations.

Document compliance status. Report compliance risks to management.