MIS761
Cyber Security Strategies

Dept. of Information Systems & Business Analytics

Deakin Business School

Week 5 – Risk Management

DEAKIN
BUSINESS SCHOOL

AACSB
ACCREDITED

Risk Tolerance and Risk Appetite

- **Risk Appetite**
  - Reflects the organization’s overall willingness to take on risk.
  - More strategic and aligns with organizational objectives and stakeholder expectations.
  - Includes a formal risk appetite statement approved by the board.
- **Risk Tolerance**
  - Defines acceptable risk levels for specific initiatives or activities.
  - More tactical and operational in nature.
  - Helps guide decisions at a granular level.
- **Residual Risk**
  - Risk that remains after all controls are applied.
  - Organizations must decide if they can accept this level of risk.
  - Documented for future review cycles.

Characteristics of a Well-Defined Risk Appetite

- **Strategic Alignment**: Risk appetite should align with organizational objectives, business plans, and stakeholder expectations.
- **Holistic Perspective**: It must encompass all key business aspects, acknowledging the willingness and capacity to take on risk.
- **Resource Consideration**: A risk appetite statement should be formally documented, considering skills, resources, and technology needed to manage risk.
- **Quantifiable Tolerance**: Include a tolerance for loss or negative events that can be reasonably quantified.
- **Periodic Review**: Regularly review and adjust risk appetite based on evolving industry and market conditions.

Overview of the Risk Management Process

- **Risk Assessment**
  - **Risk Identification:** Determining where risks are present and what specific risks exist.
  - **Risk Analysis :** Assessing the severity and impact of identified risks.
  - **Risk Evaluation :** Evaluating whether the current risk level is acceptable.
- **Risk Treatment :** Deciding on actions needed to reduce risk to an acceptable level.

Preparation in the Risk Management Process

External Context

- **Business Environment**
  - Impact of customers, suppliers, and competitors on risk management.
- **Legal and Regulatory Environment**
  - Influence of laws, regulations, and industry standards.
- **Threat Environment**
  - Awareness of threats, known vulnerabilities, and attack methods.
- **Support Environment**
  - Role of government agencies, professional associations, and service organizations.

Internal Context

- **Governance Structure**
  - Influence of the organization's governance on risk management.
- **Internal Stakeholders**
  - Impact of stakeholders within the organization.
- **Organizational Culture**
  - How the organization’s culture affects risk management processes.
- **Information Security Maturity**
  - The maturity level of the organization’s information security program.
- **Experience in Risk Management**
  - Previous experience in policy, planning, and managing risks.

Risk Identification
- Identifying Information Assets

- **Information Assets**
  - Assets that collect, store, process, or transmit information.
  - Including but not limited to people, procedures, data, software, hardware, and network components
- **Inventory Creation**
  - Avoid assigning value to assets at this stage; focus on comprehensive identification.
  - Focus on core applications first, then include communications software, operating systems, supporting utilities, and finally physical assets.
  - Distinguish between easily replaceable components like hardware and operating systems, and more critical, integral, irreplaceable information assets.

Risk Identification
- Classifying and Categorizing Information Assets

- **Purpose:** Helps prioritize protection efforts and allocate resources effectively.
- **Developing a Classification Scheme**
    - Create or review a data classification system that ranks assets by sensitivity and security requirements.
- **Common Classification Levels**
    - **Confidential:** Highly sensitive information requiring strict access control.
    - **Internal:** Information meant for internal use, with moderate security needs.
    - **Public:** Information that can be openly shared with minimal security requirements.
- **Comprehensive and Exclusive Categories**
    - Ensure every asset fits into one of the categories.
    - Each asset should belong to only one category, preventing overlap.

Risk Identification
- Assessing the Value of Information Assets

- **Prioritization**
  - Prioritize assets to ensure the most valuable ones are protected first.
  - Focus on criticality to organizational success and impact of potential loss.
- **Critical Questions for Assessment**
  - Which asset is crucial for organizational success?
  - Which asset generates the most revenue?
  - Which asset is the most profitable?
  - Which asset is most costly to replace or protect?
  - Which asset's loss would cause the greatest embarrassment or liability?
- **Valuation Challenges**
  - Value varies within and between organizations.
  - Difficult to accurately determine true value.
  - Some costs are straightforward; others, like market share loss, are hard to quantify.

Risk Identification
- Assessing the Value of Information Assets

- **Operational Costs**
  - **Creation Cost**: Value based on the cost of creating or acquiring the asset.
  - **Maintenance Cost**: Significant portion of total cost involves maintenance.
  - **Replacement Cost**: Human and technical resources needed for reconstruction or restoration.
  - **Provision Cost**: Cost of providing the asset to users.
- **Complex Valuations**
  - **Owner's Value**: Value perceived by the owners, considering the potential cost of loss.
  - **Intellectual Property**: Value of trade secrets and new product potential.
  - **Productivity Loss**: Cost of lost employee time and alternatives when assets are unavailable.
  - **Revenue Loss**: Financial impact during the period the asset is unavailable.

Risk Identification
- Using a weighted table analysis for ranking Information Assets

Asset	Criteria 1 Critical to Success	Criteria 2 Cost to Replace/Protect	Criteria 3 Public Image	Weighted Score
Criterion weight (1-100)	40	30	30	100
Customer Payment System	0.7	0.7	0.9	76
Online Order Management	0.7	0.5	0.8	67
Customer Loyalty Data	0.8	0.8	1	86

Risk Identification
- Identifying, Assessing, and Prioritizing Threats

Key Questions for Threat Identification

- **Assessing Actual Threats**
  - Determine which threats pose real danger to current information assets.
  - Focus only on threats relevant to existing software and hardware.
- **Internal vs. External Threats**
  - Identify and categorize threats as internal or external.
- **Evaluating Probability and Impact**
  - Assess which threats are most likely to occur.
  - Determine the probability of a threat’s success and its potential impact.
- **Preparedness and Response**
  - Identify threats the organization is least equipped to handle.
  - Consider the cost of protection and recovery for each threat.

Risk Identification
- Identifying, Assessing, and Prioritizing Threats

Contextual Considerations

- **Adapting to Changes**
  - Reevaluate threats when introducing new technologies or business ventures.
  - Understand new competitive and threat environments related to organizational changes.
- **Cost Analysis**
  - Prioritize threats based on the cost of protection and recovery.
  - Focus resources on managing the most expensive and impactful threats.

Risk Identification
- Using Threats-Vulnerabilities-Assets worksheet

	Customer Loyalty Data	Customer Payment System	Online Order Management
Phishing Attack	Lack of staff awareness	Employee susceptibility	N/A
Data Breach	Unsecured storage	N/A	Weak password policies
Malware	Outdated security protocols	Unpatched software	Vulnerable third-party plugins
Insider Threat	Unauthorized access	Privileged access misuse	Inadequate monitoring

Risk Analysis
- Likelihood of a Threat Event and Uncertainty

- **Focus on Unmanaged Vulnerabilities**
  - Set aside fully controlled vulnerabilities.
  - Estimate control effectiveness for partially managed vulnerabilities.
  - Assess based on implemented security controls and their levels.
- **Estimating Likelihood**
  - Combine probability of threat initiation and impact.
  - For adversarial threats: consider intent, capability, and targeting.
  - For non-adversarial threats: use historical data and empirical evidence.
  - Understand that estimation errors are inevitable.
  - Continuously refine estimates with new data and insights.
- **Incorporating Uncertainty**
  - Acknowledge the limits of knowledge on vulnerabilities and impacts.
  - Factor in uncertainty using managerial judgment and experience.

Risk Analysis
- Assessing Potential Impact

- **Impact Assessment**
  - Analyze consequences of successful attacks.
  - Focus on potential loss of asset value.
- **Scenario Creation**
  - Develop multiple scenarios to understand various impact levels.
    - Refer to media reports on similar attacks in other organizations.
    - Apply lessons learned from these cases to improve impact assessment.
  - Use a "worst case/most likely outcome" approach:
    - Speculate worst possible outcome with current protections.
    - Determine the most likely outcome.
- **Documentation and Planning**
  - Document risk impacts for all threats, vulnerabilities, and assets (TVA).
  - Use this information for contingency planning, incident response, disaster recovery, and business continuity.
    - Share assessment details with the contingency planning team.
    - Integrate findings into broader organizational planning activities.

Risk Analysis
- Using Risk Rating Worksheet for Risk Determination

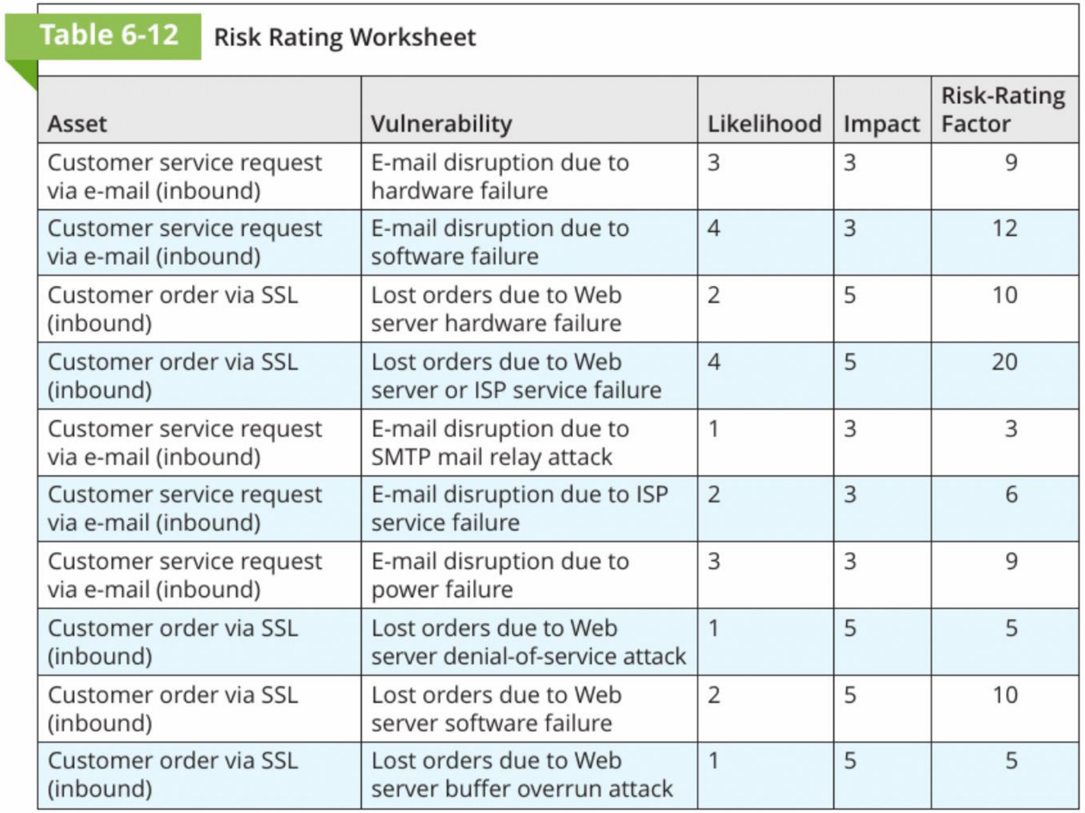

Table 6-12 Risk Rating Worksheet

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
Customer service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
Customer order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20
Customer service request via e-mail (inbound)	E-mail disruption due to SMTP mail relay attack	1	3	3
Customer service request via e-mail (inbound)	E-mail disruption due to ISP service failure	2	3	6
Customer service request via e-mail (inbound)	E-mail disruption due to power failure	3	3	9
Customer order via SSL (inbound)	Lost orders due to Web server denial-of-service attack	1	5	5
Customer order via SSL (inbound)	Lost orders due to Web server software failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server buffer overrun attack	1	5	5

- **Risk Determination Formula**
  - Calculate risk as Likelihood × Impact.
  - Incorporate uncertainty if necessary, though often simplified.
- **Purpose of the Worksheet**
  - Summarizes risk analysis results.
  - Prioritizes assets based on their risk rating.

Risk Evaluation

- **Translating Risk Appetite**
  - Convert the general risk appetite statement into numerical values.
  - Compare these values to the analyzed risks for decision-making.
  - Incorrect evaluation can leave key assets exposed.
- **Executive Decision Making**
  - Review analysis findings with governance groups and executives.
  - Decision makers determine if the risk level is acceptable.
  - If acceptable, move to monitoring and review. If not, proceed to risk treatment.
- **Complexity and Interdependencies**
  - Solutions for one asset may affect others positively or negatively.
  - Example: Upgrading a firewall can be costly but beneficial across assets.
  - Example: Simplifying a firewall might ease management but expose other assets.

Risk Treatment Strategies- Defense

- **Reducing Likelihood of Attack**
  - Improve asset security to lower the chances of successful threats.
  - Achieve an acceptable level of residual risk aligned with the organization's risk appetite.
- **Key Approaches**
  - **Policy Implementation**
    - Mandate procedures through organizational policies.
    - Combine policy changes with employee training and technology application.
  - **SETA Programs**
    - Enhance security through education, training, and awareness programs.
    - Ensure employees understand and comply with security policies.
  - **Technological Controls**
    - Use technical safeguards to reduce risks effectively.
    - Implement advanced security technologies to protect information assets.

Risk Treatment Strategies- Transference

- **Shifting Risks**
  - Transfer risk to other entities or areas.
  - Options include outsourcing services, revising deployment models, purchasing insurance, or using service contracts.
- **Effective Service Level Agreements (SLAs)**
  - Crucial for ensuring external entities meet required security levels.
  - Key SLA elements:
    - Service category (e.g., availability, response time)
    - Acceptable service quality range
    - Measurement definitions and formulas
    - Credits/penalties for performance
    - Measurement frequency and intervals

Risk Treatment Strategies- Mitigation

- **Reducing Impact with Planning and Preparation**
  - Focuses on minimizing consequences if a vulnerability is exploited.
  - Emphasizes readiness to handle incidents or disasters.
- **Types of Mitigation Plans**
  - Incident Response (IR) Plan
  - Disaster Recovery (DR) Plan
  - Business Continuity (BC) Plan
  - Crisis Management (CM) Plan

Risk Treatment Strategies - Acceptance and Termination

Acceptance

- **Intentional Decision, Not Neglection**
  - Choose to maintain current protection levels after formal evaluation.
  - Accept potential outcomes of vulnerabilities without additional controls.
- **Criteria for Acceptance**
  - Assess the risk level to the information asset.
  - Evaluate the probability and impact of an attack.
  - Conduct a feasibility analysis and financial assessment (e.g., CBA).
  - Determine that the cost of additional controls exceeds their benefits.

Termination

- **Removing Assets, Not Abandonment**
  - **Discontinue** or **remove** information assets that are too costly or difficult to protect.
  - Ensure termination is a deliberate business decision, **NOT abandonment**.
- **Cost-Benefit Analysis**
  - Decide based on the comparison of protection costs against the asset's value.

Risk Treatment
- Selecting a Strategy

General Guidelines for Strategy Selection

- **Implement Controls:** For critical assets with vulnerabilities, apply security measures to reduce exploitation likelihood.
- **Layered Protections:** When vulnerabilities are exploitable, use multiple layers of protection, including design and administrative controls.
- **Increase Attacker Costs:** If attacker's gain outweighs attack costs, use technical and managerial controls to raise attack costs or reduce attacker gains.
- **Limit Potential Loss:** For substantial potential losses, employ design principles and protections to minimize attack impact and reduce loss potential.

Comprehensive Assessment

- Analyze both economic and noneconomic consequences of vulnerability exploitation.
- Consider legal or regulatory requirements for protecting sensitive information.
- Compare actual and perceived advantages of implementing controls against disadvantages.
- Ask: "Is further investment in protection worth the cost?"

Risk Treatment
- Selecting a Strategy: Economic Feasibility

- **Cost Considerations**
  - **Development or Acquisition**: Costs for hardware, software, and services.
  - **Training Fees**: Expenses for personnel training.
  - **Implementation Costs**: Expenses for installing, configuring, and testing.
  - **Service Costs**: Vendor fees for maintenance, upgrades, or outsourcing.
  - **Maintenance Costs**: Labor expenses for ongoing verification, maintenance, training, and updates.
  - **Potential Loss Costs**: Costs from asset loss due to termination or compromise.
- **Benefit Assessment**
  - Determine the value of using controls to prevent losses.
  - Value information assets exposed by vulnerabilities.
  - Calculate risk level and express potential losses as Annualized Loss Expectancy (ALE).

Risk Treatment
- Selecting a Strategy: Cost-Benefit Analysis (CBA)

Single Loss Expectancy (SLE) Calculation

- SLE = Asset Value (AV) × Exposure Factor (EF)
  - EF represents the percentage loss from a specific attack.
  - SLE accounts for the asset value and expected loss percentage.

Annualized Loss Expectancy (ALE) Calculation

- ALE = SLE × ARO
  - ARO indicates the frequency of attacks over a given time period.
  - ALE combines SLE with ARO to estimate annual loss potential.
- **Cost-Benefit Analysis (CBA) Calculation**
  - Compare ALE before and after implementing controls.
  - CBA = ALE (pre-control) - ALE (post-control) - Annualized Cost of Safeguard (ACS)
  - Pre-control ALE is the risk before implementing the control.
  - Post-control ALE is the risk after the control has been in place.
  - ACS includes costs for implementing and maintaining the control.

Risk Treatment
- Selecting a Strategy: Other Feasibility

Organizational Feasibility

- Assess how well the InfoSec alternatives support the organization’s efficiency and strategic objectives.
- Ensure the proposed controls align with the organization's mission and goals without hindering opportunities.

Operational Feasibility (Behavioral Feasibility)

- Gauge user and management acceptance and support.
- Evaluate system compatibility with stakeholder requirements.
- Foster user engagement through communication, education, and involvement to reduce resistance to change.

Risk Treatment
- Selecting a Strategy: Other Feasibility

Technical Feasibility

- Determine if the organization has or can acquire the necessary technology.
- Assess the organization's technical expertise to manage and implement new controls.
- Consider the complexity of technological controls and the organization’s capacity to support them.

Political Feasibility

- Analyze the consensus and relationships within the organization’s communities of interest.
- Ensure proposed controls fit within the realm of what is politically possible, considering staff resources and organizational dynamics.

Risk Treatment
- Selecting a Strategy: Alternative Models

Benchmarking

- Compare organizational performance against established measures.
- **External Benchmarking**: Study practices of other organizations to achieve desired results.
- **Internal Benchmarking (Baselining)**: Compare past performance (baseline) with current performance to identify gaps and plan improvements.
- Use metrics-based or process-based measures for comparisons.

Due Care and Due Diligence

- Ensure the organization meets minimum security standards.
- Reflect actions any prudent organization would take under similar circumstances.

Risk Treatment
- Selecting a Strategy: Alternative Models

Best Business Practices

- Implement industry-recognized practices balancing information access and protection.
- Aim for effective security without compromising operational needs.

Gold Standard

- Aspire to set the highest industry standards beyond best practices.
- Pursue exemplary security measures to lead the industry.

Government Recommendations and Best Practices

- Follow regulatory requirements and recommendations specific to the industry.
- Utilize government guidelines as benchmarks for controlling InfoSec risks.

ENJOY YOUR BREAK!

SEE YOU ON AUG 20

CRICOS Provider Code: 00113B

AACSB ACCREDITED

DEAKIN BUSINESS SCHOOL

DEAKIN UNIVERSITY AUSTRALIA Worldly