

Lesson 19

Summarizing Risk Management Concepts

Topic 19A

Explain Risk Management Processes and Concepts

Syllabus Objectives Covered

- 5.4 Summarize risk management processes and concepts

Risk Management Processes

- Phases of risk management
 1. Identify mission essential functions
 2. Identify vulnerabilities
 3. Identify threats
 4. Analyze business impacts
 5. Identify risk response
- Risk assessment
 - Likelihood and impact
- Enterprise risk management (ERM) frameworks
- Risk and control self-assessment (RCSA)
- Risk and control assessment (RCA)

Risk Types

- External
 - Cyber threat actors and natural or person-made disaster
- Internal
 - Risks that arise from assets that are owned/managed
- Multiparty
 - Ripple impacts in the supply chain
- Intellectual property (IP) theft
- Software compliance/licensing
 - Shadow IT
- Legacy systems













Quantitative Risk Assessment

- Quantitative versus qualitative assessments
- Concrete values to risk factors
 - Single Loss Expectancy (SLE)
 - Exposure Factor (EF)
 - Annualized Loss Expectancy (ALE)
 - Annualized Rate of Occurrence (ARO)
- Difficulty of forecasting likelihood
- Difficulty of assessing impact/cost



Image © 123RF.com.

Qualitative Risk Assessment

Risk Factor	Impact	ARO	Cost of Controls	Overall Risk
Legacy Windows Clients				
Untrained Staff				
No Antivirus Software				

- Seeks opinions and uses broad categorizations
- Heat map or traffic light impact matrix
- Security Categorizations (FIPS 199)
 - Low
 - Medium
 - High

Risk Management Strategies

- Inherent risk
 - Level of risk before any type of mitigation has been attempted
- Risk posture and prioritization
 - Regulatory requirements
 - High value asset, regardless of threat likelihood
 - Threats with high likelihood
 - Procedures, equipment, or software that increase the likelihood of threats
 - Return on Security Investment (ROSI)
- Risk mitigation/remediation
 - Deploy countermeasure
 - Reduce likelihood or impact or both

Risk Avoidance and Risk Transference

- Avoidance
 - Stop doing the risky activity
- Transference
 - Assign risk to a third-party
 - Cybersecurity insurance
 - Limits to transference

Risk Acceptance and Risk Appetite

- Risk acceptance/tolerance
 - Risk is assessed and monitored, but no countermeasure is put in place
 - Do not ignore risk
- Residual risk
 - Likelihood and impact after mitigation
- Risk appetite
 - Willingness to tolerate a certain level of risk
 - Established at an organization or project level
- Control risk
 - Loss of countermeasure effectiveness over time

Risk Awareness

- Communicate risk factors to stakeholders
- Risk registers
 - Risk matrix/heat map
 - Graphs
 - Relevance to workflows

Topic 19B

Explain Business Impact Analysis Concepts

Syllabus Objectives Covered

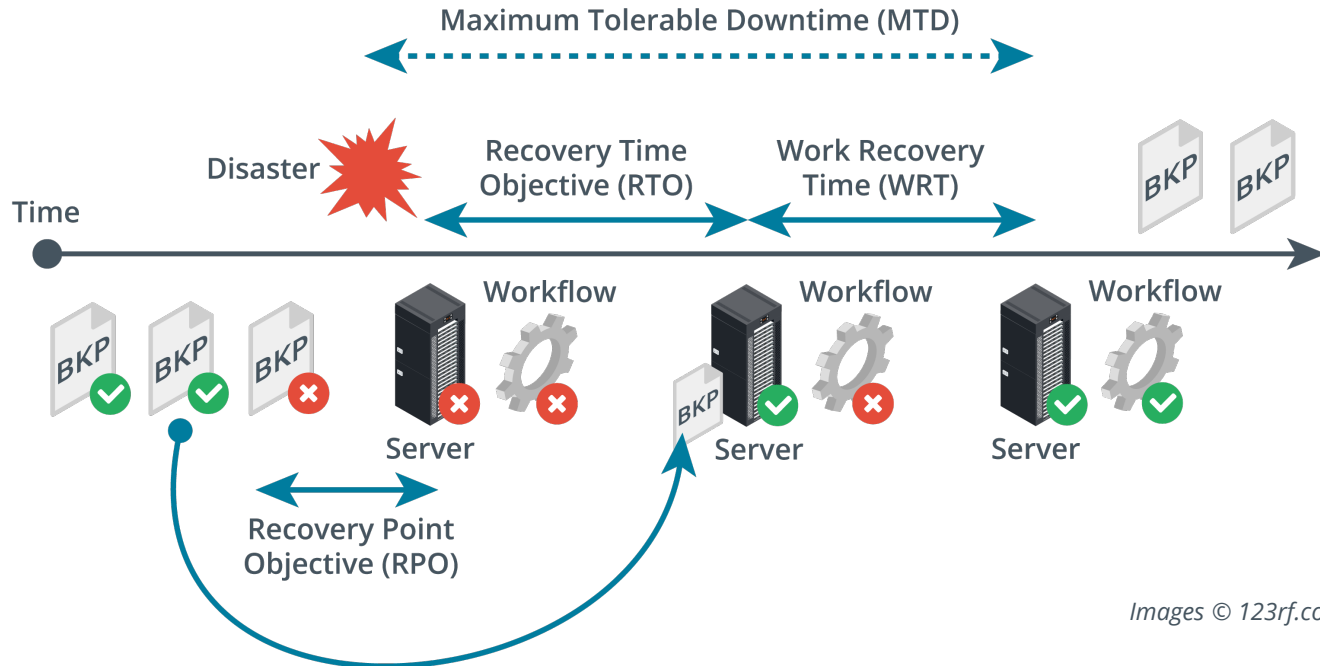
- 5.4 Summarize risk management processes and concepts

Business Impact Analysis

- Business impact analysis (BIA) reports for threat scenarios
 - Calculate impact as costs
 - Justifies and prioritizes investment in security controls
- Business continuity planning/continuity of operations planning (COOP)
 - Identifies controls and processes that maintain critical workflows

Mission Essential Functions

- Business activities that cannot be deferred
 - Contrast primary business functions (PBF)
- Metrics



Images © 123rf.com.

Identification of Critical Systems

- Supporting asset types
 - People, tangible assets, intangible assets, procedures
- Business process analysis (BPA)
 - Inputs
 - Hardware
 - Staff and other resources
 - Outputs
 - Process flow

Single Points of Failure

- Asset that causes the entire workflow to fail if it is damaged or otherwise not available
- Mean time to failure (MTTF) and mean time between failure (MTBF)
 - Determine how likely failures are to occur
 - Provision redundancy
- Mean time to repair (MTTR)
 - Time to correct fault
 - Affects recovery time objective (RTO)

Disasters

- Internal versus external
 - Whether or not threat actor/source has privileged access
 - External disasters affecting supply chain
- Person-made
 - Internal or external disaster due to human agency
 - Malicious or accidental
- Environmental
 - Could not be prevented by human agency
- Site risk assessment
 - Risk from natural disaster
 - Resiliency of utility supply
 - Health and safety risks

Disaster Recovery Plans

- Identify specific scenarios for disaster-level incidents
 - Risk and cost assessment
 - Threat modeling
- Identify tasks, resources, and responsibilities for response
- Train staff in disaster recovery and change management
- Notifications to stakeholders and agencies

Functional Recovery Plans

- Demonstrate effectiveness through walkthroughs and exercises
- Walkthroughs, workshops, and orientation seminars
 - Presentation and description-oriented
- Tabletop exercises
 - Facilitator-led discussion scenarios
- Functional exercises
 - Action-based engagements using simulations
- Full-scale exercises
 - Action-based engagements simulating major events
 - More typical of public agencies

Lesson 19

Summary

