RISK AND RESILIENCY BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK SCENARIOS

In this module we will

- Introduce the concept of a risk scenario
- Identify where risk scenarios fit into risk and resilience management

RISK SCENARIO

- A structured “story”
  - Describes how a threat could exploit a vulnerability to harm an asset
  - with stated causes, frequency/likelihood, and business impact
  - ISACA treats risks as loss event scenarios
  - This means scenarios are a fundamental unit of analysis for evaluating and responding to risk
- Resilience
  - DRI recommends building and exercising scenarios
  - To drive preparedness, continuity strategies, and testing
  - Including worst-case disaster scenarios
  - Similar to disaster drills in other industries

STEP BY STEP

- Choose the asset/service and objective at risk
  - Example: Online banking platform
  - Objective at risk: secure, available service
- State the combination of threat, actor and event
  - Example: External criminal uses credential stuffing to gain account access
- Name the vulnerability/predisposing conditions
  - Example:
    - Weak password hygiene
    - No MFAand
    - Insufficient rate-limiting for login attempts
- Describe the initiating causes and pathways
  - Example: Leaked credentials from third-party breach and automated botnet attempts

STEP BY STEP

- Estimate frequency or likelihood
  - Use qualitative scales or FAIR quantitative estimation where data allows
- Estimate business-focused impact
  - Financial loss, regulatory penalties, downtime, customer churn, reputation
- List existing controls and control strength
  - Preventive, detective, corrective
  - Take note of the residual risk
- Define response and resilience actions
  - Risk response (avoid/mitigate/transfer/accept)
  - Recovery objectives, exercises, and communications

STEP BY STEP

- Structure summary
  - Scenario title
  - Asset / business objective
  - Threat actor / path
  - Vulnerabilities / predisposing conditions
  - assumptions AND data sources
  - Likelihood
  - Impact: financial, regulatory, operational, reputation
  - Existing controls and gaps
  - Proposed treatments controls or responses
  - Resilience measures: for example RTO/RPO targets
  - Scenario owner: review cadence (frequency)

BEST PRACTICES

- Be specific and business-anchored
  - Tie each scenario to a business service, KPI, or regulatory requirement.
- Use a standard structure
  - Asset → Threat/Actor → Event/Path → Vulnerability → Frequency → Impact → Controls → Treatment → Resilience actions
- Maintain a reusable scenario catalog
  - Start with COBIT/ISACA scenario libraries; tailor to your environment and keep them versioned
- Quantify when possible
  - Apply FAIR to translate high-priority scenarios into probable loss (ranges), supporting cost-benefit decisions

BEST PRACTICES

- Exercise regularly, tabletops to live drills
  - Map scenarios to continuity tests, incident response runbooks, and recovery objectives
- Link to controls and assurance
  - Explicitly reference control objectives and rate the control strength to reveal residual risk
- Refresh with threat intelligence and incidents
  - Update likelihoods/paths as the environment changes; fold in post-incident lessons learned
- Govern with cadence
  - Assign owners, review dates, and acceptance thresholds aligned to risk appetite/tolerance

FAIR QUANTITATIVE ESTIMATION

- Factor Analysis of Information Risk
  - Open standard developed by the FAIR Institute and maintained by The Open Group
  - Used for quantifying risk in financial terms, such as probable annual loss exposure
    - *"How much risk do we have, and how much should we invest to reduce it?"*
  - FAIR breaks risk into two measurable components and a calculation
    - Loss Event Frequency (LEF) – How often is a loss likely to occur?
    - Loss Magnitude (LM) – How much loss is likely to result each time it occurs?
    - Annualized Loss Exposure (ALE) = LEF × LM
  - Replaces vague qualitative labels like "high impact" with probability ranges and financial outcomes

HOW TO USE FAIR

- Step 1: Define the scenario
  - Start with a clearly stated risk scenario
    - For example: “External attacker exploits unpatched vulnerability in web server, leading to data breach.”
- Step 2: Gather inputs
  - Use data from
    - Historical incidents and threat intelligence
    - Industry benchmarks
    - Expert judgment
  - Estimate ranges for frequency and impact
    - Minimum, most likely and maximum

HOW TO USE FAIR

- Step 3: Model and simulate
  - Monte Carlo simulation (10,000+ iterations) to combine frequency and impact distributions and produce a probable loss range
  - This produces results like
    - Most likely annual loss: $600,000
    - 90% confidence range: $250,000 – $1.2M
  - Tools like RiskLens, OpenFAIR Analysis Tool, or Python @Risk packages automate this
- Step 4: Compare controls or scenarios
  - Quantify how much each control reduces exposure
    - For example: adding MFA reduces event frequency by 70%
    - Annual loss drops from $1M to $300K
    - ROI = $700K reduction / $50K control cost = 14×

EXAMPLE: FAIR IN PRACTICE

FAIR Component	Definition	Examples / Inputs
Threat Event Frequency (TEF)	How often a threat agent acts (attempts, attacks, or hazardous events)	# of phishing campaigns per year
Vulnerability (Vuln)	Probability that an event results in loss (how effective are defenses?)	% of successful phishing attempts
Loss Event Frequency (LEF)	Expected number of loss events per year = TEF × Vuln	5 events/year
Primary Loss Magnitude (PLM)	Direct losses: recovery costs, fines, downtime	$150,000 per incident
Secondary Loss Magnitude (SLM)	Indirect losses: reputation, customer churn, legal fees	$50,000 per incident
Total Loss Magnitude (LM)	PLM + SLM	$200,000 per incident
Annualized Loss Exposure (ALE)	LEF × LM	5 × $200,000 = $1,000,000/year

EXAMPLE: FAIR IN PRACTICE

Scenario	External ransomware attack on file server
Threat Event Frequency (TEF)	12 attempts/year
Vulnerability (Vuln)	0.2 (20% likely to succeed)
LEF	12 × 0.2 = 2.4 successful events/year
Loss Magnitude (LM)	$250,000 per incident
Annualized Loss Exposure (ALE)	2.4 × $250,000 = $600,000/year
Control Implemented	Immutable backup and EDR
New Vulnerability (Vuln)	0.05 (5% success rate)
New ALE	12 × 0.05 × $250,000 = $150,000/year
Risk Reduction	$450,000 saved per year

RELATED TOOLS

- Risk scenarios, use cases, and user stories

Concept	Primary Use	Alignment
Risk Scenario	Describes a potential adverse event that could impact business objectives.	ISACA Risk IT / DRI Resilience
Use Case	Describes how a system behaves under specific conditions to achieve a goal.	System Design / Requirements
User Story	Captures a specific user interaction or requirement in agile development.	Agile / DevOps / QA

Together, they form a **continuum** — from **risk identification** to **resilience validation**.

RELATED TOOLS

- Risk scenarios extend use cases and user stories by adding the failure and resilience dimension

Aspect	Use Case	User Story	Risk Scenario
Focus	System behavior	User value	Threat impact and resilience
Question answered	"How should it work?"	"What does the user need?"	"What could go wrong?"
Owner	Business analyst / designer	Product owner / team	Risk, QA, or resilience engineer
Validation method	Functional test	Acceptance test	End-to-end risk/resilience test
Example artifact	UML use case diagram	Agile backlog item	Risk register scenario

FROM RISK TO TEST

- Start with a risk scenario
  - “Payment service unavailable due to API timeout”
- Map to use case
  - “Process online payment via API”
- Identify user stories impacted
  - “As a customer, I want to complete my payment quickly”
  - “As a support agent, I want to see failed payment logs”

FROM RISK TO TEST

- Design test cases
  - *Functional test:* Does the payment succeed under normal load?
  - *Negative test:* Does the system handle API timeout gracefully?
  - *Resilience test:* Does failover to backup gateway work?
  - *Recovery test:* Are pending payments reconciled after restoration?
  - Each test ties back to a risk statement ensuring traceability from risk identification to verification

RISK SCENARIOS AND TEST CASES

- End-to-End (E2E) testing with risk lens
  - E2E tests verify complete workflows, crossing multiple systems, APIs, and data layers
  - Combined with risk scenarios, E2E testing ensures
    - Key assets (data, transactions, customer flows) are resilient under failure
    - Preventive and detective controls actually work in production-like conditions
  - Ensures recovery paths meet
    - RTO (Recovery Time Objective) requirements
    - RPO (Recovery Point Objective) requirements

RISK AND TESTING

- Best Practices
  - Map every critical use case to at least one risk scenario
  - Maintain traceability
    - Link risk register entries to user stories, use cases, and test artifacts in your ALM or QA tool
  - Use exploratory risk testing
    - Encourage testers to explore system behavior under failure or boundary conditions
  - Test controls, not just functionality
    - Validate access controls, monitoring alerts, logging, and failover triggers
  - Automate regression of high-risk scenarios
    - Use CI/CD pipelines to continuously validate resilience against known threats
  - Close the loop
    - Feed real incidents and audit findings back into the scenario catalog for future testing

Q&A AND OPEN DISCUSSION