RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK TYPOLOGY

In this module we will explore

- The taxonomy of risk categories and risk types with mapping into IT / resilience contexts
- How these risks intersect with IT, cyber, and resilience (DRII) considerations
- Classifying real-world risk scenarios into categories/types

INTRODUCTION

- Not all risks are equal
  - We need consistent categories so we can structure governance, allocate resources, monitor, and respond to events
  - The ISACA Risk IT Framework, treats “IT-related risk” as one component among other enterprise risk categories
    - For example: strategic, operational, compliance
  - Resilience thinking (DRII) views risks not just by domain but by their impact on continuity and recovery
    - Meaning the taxonomy of risks must link to resilience design

RISK CATEGORIES (ENTERPRISE-LEVEL)

- These are the “buckets” under which risks are grouped at the enterprise ERM level
  - The next slide is a standard categorization often used in ERM
  - Cross-referenced with IT examples and notes on resilience connection
- Additional categories sometimes used
  - Financial or credit risk (especially in banks) arising from credit defaults, market swings
  - Market or competitive risk: if tech investments fail to yield competitive advantage
  - External risk: natural disasters, climate, supply chain shock
- In practice, an organization may tailor or add more categories
  - Butt the core four on the next are widely used and map well into risk governance

RISK CATEGORIES (ENTERPRISE-LEVEL)

Category	Definition / Focus	IT / Security Examples	Resilience / Continuity Considerations
Strategic Risk	Risks that affect the organization's ability to achieve its long-term goals or strategy	E.g. DevOps platform choice fails; blockchain or AI investments underperform; competitor disrupts with new tech	If a strategic risk materializes, it can derail resilience planning (e.g. you bet on a tech that becomes central but fails)
Operational Risk	Risks from internal processes, systems, human error, IT operations, supply chains	System outages, human mistakes in configuration, patching failures, IT vendor failure, process gaps in security operations	These are typically the domain most directly tied to continuity and incident recovery; resilience programs often focus heavily here
Compliance / Regulatory Risk	Risk of legal or regulatory sanctions, fines, or loss due to failure to comply with laws, regulations, standards, internal policies	Non-compliance with GDPR, PCI, banking data privacy laws, or internal security policy violations	If compliance risk causes enforced shutdowns or fines, resilience must accommodate regulatory recovery (e.g. legal continuity, remediation)
Reputational Risk	Risk of loss of stakeholder trust, brand damage, loss of customer confidence	Publicized data breach, failed security response, scandal, customer data leak, negative media	Reputational damage can prolong or amplify recovery; resilience must plan for stakeholder communication, trust rebuilding, backup channels

RISK TYPES

- Risk categories are broad domains
  - Risk types are more detailed classifications of how risk can arise
  - Typically by source or nature of failure or deviation

Risk Type	Definition / Source	Examples in IT / Security	How to Manage / Monitor
Process Risk	Risks arising because processes are flawed, incomplete, or improperly executed	Change management failures, patching process breakdown, incident response process gaps, access request process missteps	Use process controls, workflow automation, checklists, reviews, monitoring metrics (e.g. process exceptions)
Product / Technology Risk	Risk inherent to a product, system, or technology asset	Software bugs, zero-day vulnerabilities, third-party library defects, insecure configurations, embedded supplier hardware defects	Use secure development lifecycle (SDLC), code reviews, vulnerability scanning, product security reviews, vendor component vetting
Business / Legal / Financial Risk	Risk from legal, contractual, financial, liability, or business model interactions	Contractual SLA breaches, vendor liability, financial loss from breach, fines, litigation, business model failure	Legal review, financial modeling, scenario analysis, hedging, liability clauses, insurance

RISK TYPES

- Sometimes we see subtypes as a result of blending
  - Legal and regulatory risk: often under “Business / Legal / Financial”
  - Technology and infrastructure risk: overlaps “Product / Technology”
  - Third-party and supplier risk: can be a composite of process, product, legal
  - Information and data risk: cross cuts confidentiality, integrity and availability
    - Often treated as a separate axis because it cuts across process/product types
- Risk types can be viewed as modes of failure with categories as domains of impact

MAPPING: CATEGORY × TYPE MATRIX

Category \ Type	Process Risk	Product / Technology Risk	Business / Legal / Financial Risk
Strategic	Flawed strategic planning processes, misaligned risk governance process	Choosing a flawed core banking platform (product)	Business model failure, regulatory fines, contract losses
Operational	Incident handling process breakdown; patch deployment steps skipped	Vulnerability in system component; hardware failure	Financial losses due to downtime, SLA penalties
Compliance	Compliance audit process failure, incomplete checks	Noncompliant software modules, data handling features	Fines, legal liability, contractual noncompliance
Reputational	Poor handling process of public disclosures	Breach of public facing product, defacement, leaks	Legal lawsuits, customer compensation, brand loss

FROM ISACA

- Emphasizes that IT / I&T-related risks transcend categories
  - A risk might be operational, strategic, or compliance in nature depending on context
  - Each risk must be mapped into the enterprise risk taxonomy rather than being managed in isolation
- Describes risk scenario construction
  - Evaluates asset, threat, event, vulnerability, impact
  - Helps classify risk type and category more precisely
- Recommends aligning IT risk management with ERM
  - Ensures that categories and types are consistent across the enterprise

RESILIENCE PERSPECTIVE

- DRI emphasizes resilience more than taxonomy
  - Glossary for Resilience defines key resilience terms
    - “Acceptable risk,” “impact tolerance,” “capability loss”
    - Links into risk classification work.
  - Risk categories are often mapped to critical functions and their exposures
    - For example: how strategic, operational, compliance, or reputational risks threaten continuity of key services
  - Classifying risk types helps in BIA, risk assessment, and response planning
  - DRII’s annual risk and resilience trends report highlights common operational and emerging risks
    - Serves as de facto risk categories in practice
    - For example: cyber events, IT disruptions, reputational issues

RISK TYPES

- Process risks
  - Arise from failures or inefficiencies in internal business or IT processes
  - Examples
    - Ineffective change management leading to deployment errors
    - Manual data entry processes causing transaction inaccuracies
    - Poorly defined incident escalation procedures delaying recovery
  - Impact
    - May cause operational disruptions, reduced service quality, or compliance violations
  - Mitigation and resilience practices
    - Implement process standardization through Standard Operating Procedures (SOPs)
    - Embed control checkpoints and automated validations
    - Regularly test recovery and continuity procedures to ensure process resilience
    - Use continuous improvement and root cause analysis (RCA) to strengthen weak processes

RISK TYPES

- Product risks
  - Associated with the design, development, quality, or delivery of a product or service
  - Includes software quality, security vulnerabilities, and service reliability
  - Examples:
    - Defective software releases impacting customer experience
    - Unpatched vulnerabilities in customer-facing applications
    - Inadequate testing during product lifecycle phases
  - Impact
    - Loss of customer trust, reputational damage, or financial penalties
    - For example: service downtime or noncompliance
  - Mitigation and resilience practices
    - Apply QA and DevSecOps practices throughout the product lifecycle
    - Perform risk-based testing (RBT) to prioritize testing of high-impact areas
    - Use configuration management to track and control software versions
    - Maintain rollback and failover mechanisms for resilience during releases

RISK TYPES

- Business risks
  - Affect the organization’s ability to achieve strategic, financial, or regulatory objectives
  - Often arise from the external environment
    - For example: market, competitors, legislation changes
  - Or from internal governance and decision-making weaknesses
    - For example: overestimating the organization’s capability or ignoring market data and analyses
    - For example: incompetent executives or toxic work environments

RISK TYPES

- Business risk subtypes

Subtype	Examples	Potential Impact	Mitigation / Resilience Practice
Legal Risk	Noncompliance with data privacy laws (e.g., GDPR, HIPAA)	Fines, sanctions, loss of trust	Regular audits, legal reviews, compliance automation
Financial Risk	Budget overruns, currency fluctuations, poor investment	Cash flow issues, loss of profitability	Financial controls, forecasting, diversification
Strategic Risk	Poor alignment between IT projects and business goals	Lost market opportunities	Portfolio management, balanced scorecard
Reputation Risk	Negative publicity from data breaches	Customer loss, reduced brand value	Transparent communication, robust incident response
Human Resource Risk	Loss of critical staff or poor succession planning	Operational delays	Workforce resilience planning, knowledge management

CORRELATIONS

- Asset
  - Anything of value to the organization
    - Financial assets
    - Information
    - Business and supporting processes
    - Infrastructure
    - People
    - Reputation
  - Risk = Threat × Vulnerability × Asset Value
    - This is a refinement of the terminology from before
    - The outcome can be thought of as the negative impact on the value of an asset
    - Without an asset to protect, there is no risk
    - Without a vulnerability, threats have no entry point
    - Without a control, the risk remains unmitigated

CORRELATIONS

- Correlations
  - *Assets* are protected by *Controls*
  - *Assets* are exposed via *Vulnerabilities*
  - *Vulnerabilities* are exploited by *Threats*
  - Exploited *Vulnerabilities* are *Risk Events*
  - *Risk Events* reduce the value of *Assets*

EXAMPLE

- A bank's customer facing banking interface
  - *Asset*: Online banking platform
    - Question: What sort of asset is this? Can it represent more that one actual asset?
  - *Threat*: Cybercriminal attempts to use stolen credentials
  - *Vulnerability*: Weak password policy and lack of two-factor authentication
  - *Risk*: Unauthorized access to customer accounts
  - *Control*: Implement MFA, monitor failed login attempts, perform security testing

INTEGRATION

- Integration with risk management lifecycle
  - Both ISACA and DRI emphasize continuous improvement
    - Identify assets and threats
    - Assess vulnerabilities and risks
    - Design and implement controls
    - Monitor effectiveness and adapt
    - Review after incidents for continual improvement
  - Continuous feedback loop strengthens operational resilience

INTERNAL VS. EXTERNAL THREATS

- Internal threats
  - Internal threats originate within the organization
    - Come from employees, contractors, systems, or processes that are part of the enterprise environment
    - May be intentional (malicious actions) or unintentional (accidents, negligence, process errors)

Category	Example	Description / Impact
Human Error	Data deletion, misconfiguration, sending sensitive data to the wrong recipient	Common in IT and operations; leads to service disruption or data loss
Malicious Insider	Disgruntled employee exfiltrating data	Threatens confidentiality and reputation
Process Failures	Inadequate change management, flawed SOPs	Can cause downtime or compliance breaches
System Misuse	Privilege abuse, bypassing security controls	Compromises internal controls
Poor Security Culture	Weak password practices, social engineering success	Creates vulnerabilities that external actors can exploit

INTERNAL VS. EXTERNAL THREATS

- Internal threats
  - Key drivers (root causes) example
    - Lack of security awareness training
    - Weak role-based access control and monitoring
    - Poor process documentation and change governance
    - Inadequate separation of duties
- Mitigation and resilience strategies examples
  - Preventive controls
    - Implement least-privilege access and multi-factor authentication (MFA)
    - Conduct employee security training and periodic awareness refreshers
  - Detective controls
    - Monitor logs and behavior analytics for anomalous activities
    - Employ data loss prevention (DLP) tools
  - Corrective controls
    - Ensure backup, recovery, and version control systems are robust
    - Use post-incident reviews to strengthen process maturity

DLP TOOLS

- Data Loss Prevention (DLP) tools
  - Security solutions designed to detect, monitor, and protect sensitive data to prevent unauthorized access, leakage, or exfiltration
  - Monitors when data is in use, in motion, or at rest
- Core functions
  - Data discovery and classification
    - Scans systems, databases, and endpoints to identify sensitive or regulated data
    - For example: personal, financial, or proprietary information
    - Applies classification tags for monitoring and enforcement
    - Correlates with DAMA best practices

DLP TOOLS

- Core functions
  - Policy enforcement
    - Defines rules that restrict how sensitive data can be accessed, transferred, or shared
    - For example, blocking external email attachments containing credit card numbers
  - Monitoring and detection
    - Tracks data movements across endpoints, networks, and cloud environments to detect policy violations or unusual activity
  - Incident response and reporting
    - Alerts administrators, quarantines data, or blocks transmission when a potential data loss event occurs
    - Generates reports for compliance audits and investigations

INTERNAL VS. EXTERNAL THREATS

- External threats
  - External threats originate outside the organization’s boundaries
  - Driven by actors or forces not under the organization’s control
    - For example: cybercriminals, competitors, environmental factors, and geopolitical events
    - Often exploit vulnerabilities introduced by technology exposure, supply chain dependencies, or public-facing systems

Examples

Category	Example	Description / Impact
Cyber Threats	Phishing, ransomware, DDoS, zero-day exploits	Disruption of IT operations, data breach, financial losses
Physical / Environmental	Floods, fires, earthquakes	Physical damage to infrastructure or data centers
Third-Party / Supply Chain	Vendor outages, compromised service provider	Cascading service disruption and compliance risk
Economic / Market	Recession, inflation, market volatility	Financial strain and business model risk
Geopolitical / Regulatory	Sanctions, regulatory changes, political unrest	Compliance risk and operational disruption

INTERNAL VS. EXTERNAL THREATS

- External threats
- Key driver (root causes) examples
  - Increased exposure from digital transformation and cloud services
  - Globalized supply chains with interdependencies
  - Rapidly evolving threat landscape (e.g., AI-driven attacks)
  - Natural and geopolitical instability

INTERNAL VS. EXTERNAL THREATS

- Preventive control examples
  - Perform vendor risk assessments and due diligence
    - Implement perimeter defences, intrusion detection, and patch management
    - Design geographically diverse continuity and recovery sites
  - Detective controls
    - Continuous monitoring of external threat intelligence feeds
    - Establish Security Operations Centers (SOC) or Managed Detection and Response (MDR) partnerships
  - Corrective controls:
    - Test disaster recovery and continuity plans regularly.
    - Include supply chain resilience in risk assessments and contracts.

INTERNAL VS. EXTERNAL THREATS

Aspect	Internal Threats	External Threats
Origin	Within the organization	Outside the organization
Actor Examples	Employees, contractors, internal systems	Hackers, competitors, natural disasters
Control Level	High (organization has direct influence)	Medium to low (limited influence)
Typical Focus	Insider controls, awareness, process reliability	Perimeter security, third-party risk, environment
Detection Difficulty	Often subtle (may appear as normal activity)	Usually more visible once triggered
Resilience Planning Emphasis	Process maturity, culture, access control	Redundancy, supply chain continuity, incident response

Q&A AND OPEN DISCUSSION