RISK AND RESILIENCE BOOTCAMP

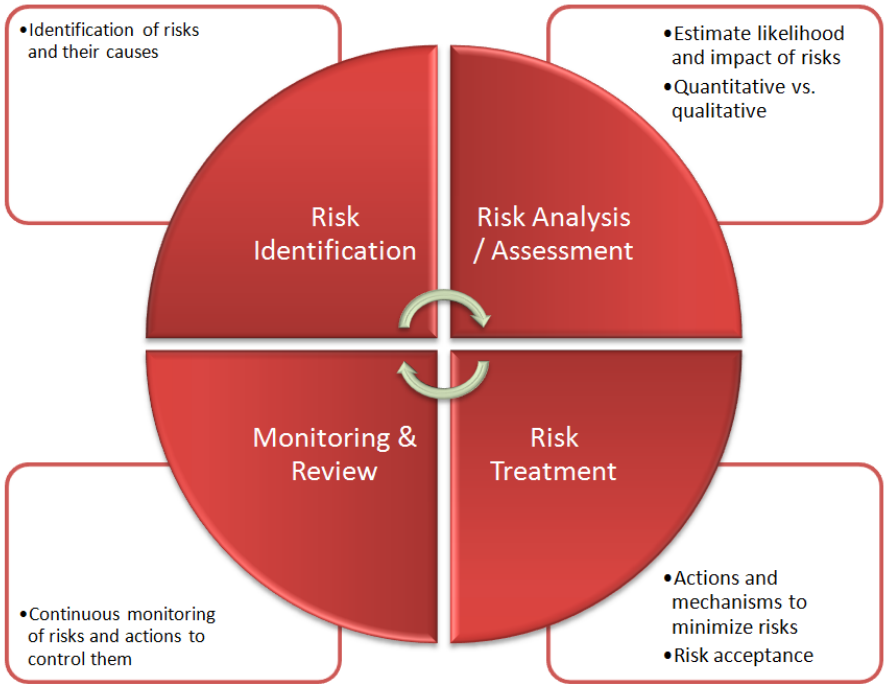
TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK STATEMENTS AND REGISTERS

In this module we will cover

- Risk Statements
- Risk Registers



RISK STATEMENTS

- Risk statements
  - Translate observations and analysis into clear, actionable form
  - Provide a common language between technical, business, and governance teams
  - Essential for prioritization, mitigation, and executive decision-making
- A strong risk statement answers the question
  - *"What could happen, why could it happen, and what would be the impact if it does?"*
  - This structure ensures that risks are complete, specific, and testable, supporting later steps in analysis and monitoring

STRUCTURE OF A RISK STATEMENT

- A standard risk statement includes three core elements
  - Sometimes called the “CPC model”
    - *Eg. “If backups are not verified weekly (condition), then a restoration may fail during a disruption (potential), resulting in data loss and prolonged service outage (consequence).”*

Element	Meaning	Example
Condition (Cause)	The existing situation, weakness, or trigger that creates risk exposure.	“If backups are not verified weekly…”
Potential (Event)	The possible incident or event that could occur because of the condition.	“…then a restoration may fail during a disruption…”
Consequence (Impact)	The negative outcome or effect on business objectives.	“…resulting in data loss and prolonged service outage.”

EFFECTIVE RISK STATEMENTS

Characteristic	Explanation / Best Practice
Specific and Concise	Avoid vague terms ("system failure") — describe the exact risk source or asset.
Objective	Base on evidence (logs, interviews, audits) — avoid assumptions.
Neutral Tone	State facts, not blame ("system misconfiguration," not "admin negligence").
Aligned with Objectives	Always tie the consequence to a business outcome (revenue, compliance, reputation, continuity).
Quantifiable when possible	Where feasible, indicate exposure in measurable terms (e.g., "potential revenue loss > $500K").
Linked to Controls	Mention related existing controls or planned mitigation — keeps the statement actionable.

COMMON MISTAKES

Weak Statement	Why It's Weak	Improved Version
"Network outage could hurt operations."	Too vague; lacks cause or measurable impact.	"If redundant internet links are not configured correctly, a regional outage could cause 6+ hours of service downtime, delaying customer transactions."
"Data might be stolen."	Missing condition and business impact.	"If multi-factor authentication is not enforced for privileged accounts, an attacker could gain unauthorized access, leading to data theft and compliance fines."
"Staff turnover risk."	Too generic; unclear link to objectives.	"If critical application administrators leave without proper handover, system maintenance may lapse, leading to extended downtime or support gaps."

INTEGRATING WITH IDENTIFICATION PROCESS

- Interviews
  - Provide the conditions (e.g., weak process)
- Logs and checklists
  - Identify the potential events
- Exploratory analysis
  - Reveals the consequences and ripple effects
- The completed statement forms the foundation for risk scoring, register entries, and mitigation plans

RISK REGISTERS

- The risk register
  - Is the organization's central, living repository for all identified risks, their analyses, mitigation plans, and monitoring status
  - Ensures that nothing discovered during risk identification gets lost and that ownership, accountability, and follow-up are visible
- Think of it as the "memory" and dashboard of risk management

CORE FUNCTIONS

Function	Description
Catalog of Risks	Consolidates all risk statements identified from interviews, logs, checklists, etc.
Accountability Tool	Assigns risk ownership and action responsibility.
Monitoring Instrument	Tracks mitigation progress, review cadence, and control performance.
Communication Platform	Provides summarized information to management, auditors, and regulators.

TYPICAL STRUCTURE AND FIELDS

Field	Purpose / Description
Risk ID	Unique identifier for traceability.
Risk Statement	"Condition → Potential → Consequence" text.
Category / Type	Operational, Compliance, Strategic, etc.
Source / Method of Identification	Interview, Log Review, Audit, etc.
Inherent Likelihood / Impact	Pre-control risk rating.
Existing Controls	Preventive, Detective, Corrective.
Residual Risk Level	After controls are applied.
Mitigation Plan / Actions	Planned remediation steps.
Risk Owner	Individual or role accountable for management.
Review Cadence / Date	Frequency of review (monthly, quarterly).
Status / Trend	Open, In-Progress, Closed; improving or deteriorating.
Last Update / Reviewer	Version control and audit trail.

“LIVING DOCUMENT” PRINCIPLE

- A risk register is not static
  - It must be continuously updated as the environment, controls, and risk appetite evolve
- Examples of updates
  - New risk identified from a security incident: added immediately
  - Control implemented: residual risk level adjusted downward
  - Business process decommissioned: related risk closed
  - Regulatory change: new compliance risks introduced

REVIEW CADENCE

Risk Severity	Review Frequency
Critical	Monthly
High	Quarterly
Medium	Semi-Annually
Low	Annually

INTEGRATION WITH OTHER PROCESSES

Process	Relationship to Risk Register
Risk Identification	Each method (interview, log, checklist) feeds new entries into the register.
Testing & QA	Provides validation evidence for controls linked to each risk.
Incident Management	Closed incidents can generate new risks or update likelihoods.
Governance Reporting	Register summaries inform dashboards for executives and auditors.
Resilience Planning	Links to BIAs, continuity plans, and recovery objectives.

SIMPLIFIED RISK REGISTER ENTRY

Field	Example
Risk ID	R-2025-004
Risk Statement	*If system patches are delayed (condition), vulnerabilities may be exploited (potential), resulting in data breach and regulatory fines (consequence).*
Category	Operational / Cyber
Inherent Likelihood	High
Inherent Impact	High
Existing Controls	Patch schedule, vulnerability scans
Residual Risk	Medium
Mitigation Actions	Automate patching; implement patch SLA alerts
Owner	IT Operations Manager
Review Frequency	Quarterly
Status	In Progress
Last Updated	2025-09-30

Q&A AND OPEN DISCUSSION