“Develop a passion for learning.”

RISK AND RESILIENCE BOOTCAMP

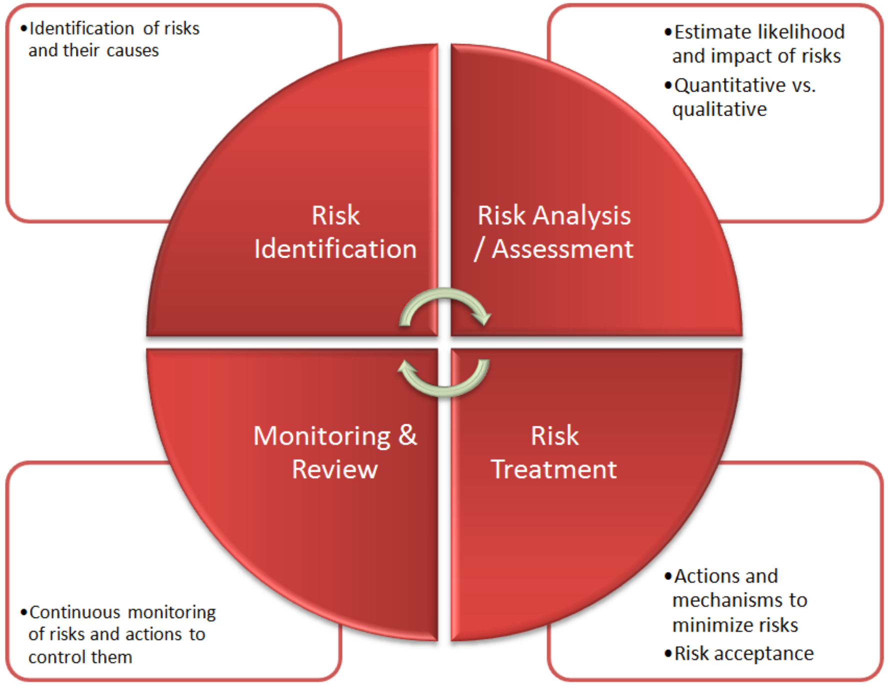
TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK IDENTIFICATION

In this module we will cover

- Risk identification methods
- Exploratory risk analysis



Risk Identification

- Identification of risks and their causes

Risk Analysis / Assessment

- Estimate likelihood and impact of risks
- Quantitative vs. qualitative

Risk Treatment

- Actions and mechanisms to minimize risks
- Risk acceptance

Monitoring & Review

- Continuous monitoring of risks and actions to control them

RISK IDENTIFICATION METHODS

- First actionable stage in the risk management lifecycle
  - Needs to happen before risk analysis, evaluation and management
  - Links directly to risk typologies
    - Operational, strategic, compliance, reputation
  - Links to risk types
    - Process, product, business/legal/financial
- Objective:
  - To identify potential events or conditions (threats, vulnerabilities, asset exposures, control gaps) that could impact business objectives or system resilience (e.g., mission-critical services, IT assets, operational processes)
  - Not a one-time activity, but should be iterative and ongoing responsive to changes in environment, technology, regulation, process, business model

RISK IDENTIFICATION METHODS

- Emergent risk identification
  - New risks may surface as systems evolve, both internal and external
  - New risks my emerge from market and social innovations, crises and changes
    - Including black swan events
- Should be comprehensive
  - Multiple viewpoints: operations, IT, vendors, third-parties, end-users
  - Essential for effective risk statements, risk registers, and subsequent risk analysis and testing

INTERVIEWS

- Preparation
  - Purpose: Ensure the interview is structured, goal-oriented, and aligned with the organization's risk framework
  - A well-planned interview minimizes wasted time and increases the reliability of findings
- Key activities
  - Define the scope
  - What part of the business or system is being reviewed?
    - Example: Customer-facing web applications, data centers, supplier onboarding.
  - What type of risk do you seek to uncover?
    - Operational, compliance, reputational, process, etc.
  - Align with risk appetite and tolerance levels already defined in the organization

INTERVIEWS

- Key activities
  - Identify target roles and stakeholders
  - Include multiple perspectives:
    - *Process owners:* know daily operations and bottlenecks
    - *System administrators or engineers:* understand control mechanisms and technical vulnerabilities
    - *Business stakeholders:* grasp business objectives, financial exposure, and customer impact
    - *Vendors or third-party partners:* identify supply-chain risks
    - *Front-line staff:* reveal practical workarounds or shadow systems
  - Balance hierarchical levels
    - Senior leaders provide strategic risks; operational staff reveal execution risks

INTERVIEWS

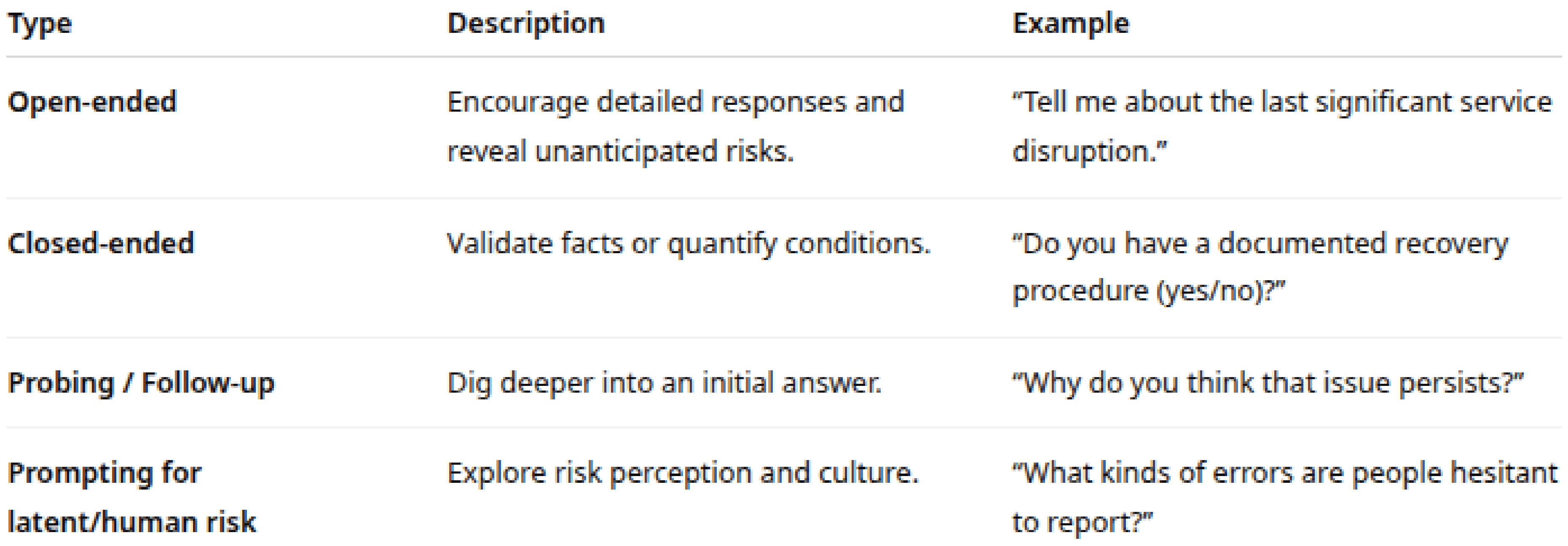
- Key activities
  - Set objectives and logistics
    - Clarify the purpose: discovery, validation, or follow-up
    - Determine interview format: one-on-one, group workshop, or panel
    - Allocate sufficient time (30–60 minutes typical)
    - Send participants a short briefing describing the purpose and assuring confidentiality
  - Best practice tip
    - Use a Risk Identification Worksheet to log participant names, domain, risk category focus, and notes

INTERVIEWS

- Designing the interview guide
  - Goal: Create a structured but flexible framework that elicits both factual and interpretive information
- Structure
  - *Opening questions:* build context
    - “Describe your role and daily responsibilities”
  - *Exploratory questions:* uncover known and latent risks
    - “What could prevent you from meeting your targets?”
  - *Analytical questions:* evaluate existing controls
    - “How do you monitor for errors or exceptions?”
  - *Reflective questions:* uncover behavioral and cultural risks
    - “Do people feel safe raising problems?”

INTERVIEWS

- Question types



Type	Description	Example
Open-ended	Encourage detailed responses and reveal unanticipated risks.	“Tell me about the last significant service disruption.”
Closed-ended	Validate facts or quantify conditions.	“Do you have a documented recovery procedure (yes/no)?”
Probing / Follow-up	Dig deeper into an initial answer.	“Why do you think that issue persists?”
Prompting for latent/human risk	Explore risk perception and culture.	“What kinds of errors are people hesitant to report?”

INTERVIEWS

- Tailoring by stakeholder role
  - *Process owners:* ask about bottlenecks, manual steps, exception handling
  - *Vendors*: ask about contract dependencies, SLA adherence, escalation procedures
  - *Business stakeholders:* focus on financial, legal, or reputational impact of disruptions
  - *Technical teams:* probe system vulnerabilities, logging, monitoring, or change-control practices
  - Deliverable: A written guide with core questions and a space for notes, ratings (e.g., likelihood/impact), and references to evidences

INTERVIEWS

- Conducting the interview
  - Purpose: Create a conversation that yields genuine insights rather than scripted answers
- Structure
  - Establishing rapport
    - Begin with introductions, confidentiality assurance, and explanation of why their input matters
    - Use neutral, non-judgmental language (“help us understand” instead of “audit” or “investigate”)
    - Demonstrate active listening: maintain eye contact, summarize answers, and check understanding
  - Capturing insights
    - Take structured notes or record (with consent)
    - Tag responses with relevant risk categories and control references
    - Pay attention to tone and emotion: hesitation or defensiveness often signals areas of concern

INTERVIEWS

- Structure
  - Probing for “hidden” risks
    - Explore shadow IT (unauthorized tools or workarounds)
    - Identify cultural or behavioral risks: lack of accountability, fear of escalation
    - Look for process gaps: missing hand-offs, unclear ownership, outdated procedures
    - Ask scenario-based prompts like
    - *“If this system failed on a weekend, what would you do?”*
    - *“How long could you continue operations manually?”*
  - Managing group dynamics
    - In workshops, prevent dominant voices from overshadowing quieter participants
    - Encourage cross-functional discussion to reveal dependencies

INTERVIEWS

- Post-interview activities
  - Purpose: Turn raw interview data into actionable risk insights
- Document findings
  - Summarize responses in a risk identification template
    - Source → Risk condition → Consequence → Existing controls → Owner → Evidence
    - Use direct quotes for strong insights (e.g., “We don’t have time to verify every nightly backup.”)
  - Synthesize into risk statements
    - Convert observations into standardized form:
    - If [condition], then [event] may occur, leading to [consequence]
    - Example: “If vendor onboarding is not independently verified, third-party access may be provisioned incorrectly, leading to data exposure.”

INTERVIEWS

- Document findings
  - Cross-check with other evidence
    - Compare interview insights against logs, incident reports, and checklists
    - Validate inconsistencies: does operational data support what people said
    - Flag contradictions for follow-up investigation.
  - Communicate findings
    - Present results to risk owners or governance committees
    - Prioritize issues for inclusion in the risk register

LOG AND DATA REVIEW

- Logs
  - Digital footprints of activities, events, and control actions across systems and processes
  - Represent how the organization's technology, people, and controls actually behave, not how they are documented to behave
- Goal is to move from raw data to meaningful patterns that may indicate risk conditions or control failures
  - Anomalies
    - Unusual patterns in access, usage, or transaction data
    - Example: Spike in failed logins outside business hours → potential brute-force attack or misconfiguration
    - Example: System restarts at irregular intervals → stability issue or unauthorized reboot

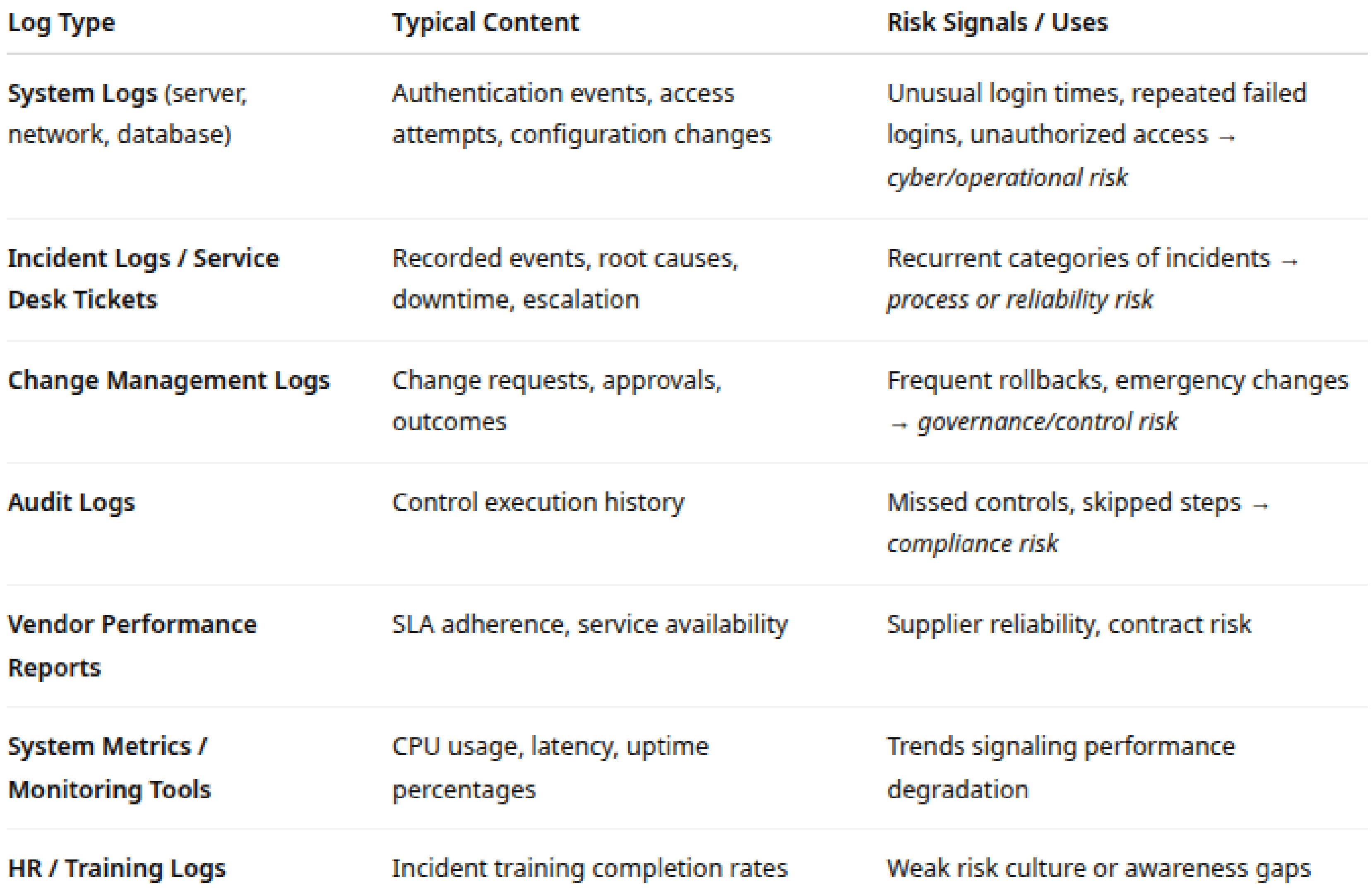
LOG AND DATA REVIEW

- Recurring events
  - Same error or alert type repeating across systems or time periods
  - Example: Monthly backup job failing → risk of data loss
  - Example: Repeated password reset requests → possible credential fatigue or phishing
- Trend patterns
  - Gradual increase or decrease in certain events or metrics
  - Example: Increasing incident resolution times suggesting staffing or skill shortage risk
  - Example: Decreasing ticket closure rate suggesting operational inefficiency
- Deviations from expected behavior
  - "Normal" baseline drift: performance metrics or logs diverge from their usual range
  - Example: Transaction volume drop without business reason suggest potential outage, process failure, or fraud
  - Example: Firewall rule count rising unexpectedly suggests configuration drift or security overcomplication

LOG AND DATA REVIEW

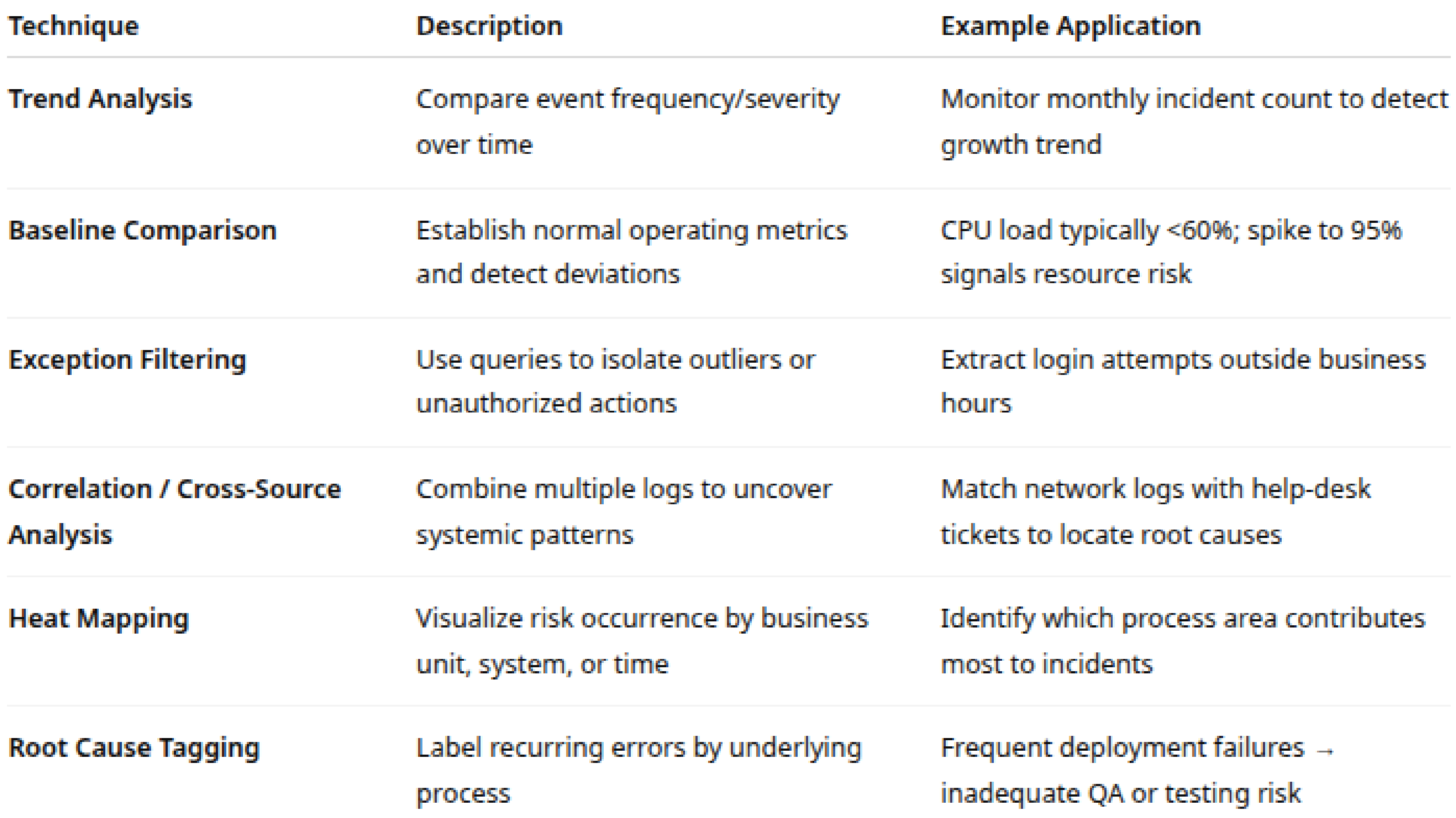
- Threshold deviations
  - SLA or KPI breaches
  - Example: Incident resolution time rises above SLA limit
- Compliance gaps
  - Missing log entries or unreviewed exceptions suggest an audit deficiency
- Advanced patterns
  - Correlated anomalies: e.g., spike in system errors + delayed customer support responses suggests combined process risk
- Silent periods
  - Absence of logs where activity is expected (indicator of failure or tampering)

TYPES OF LOGS AND DATA SOURCES



Log Type	Typical Content	Risk Signals / Uses
System Logs (server, network, database)	Authentication events, access attempts, configuration changes	Unusual login times, repeated failed logins, unauthorized access → *cyber/operational risk*
Incident Logs / Service Desk Tickets	Recorded events, root causes, downtime, escalation	Recurrent categories of incidents → *process or reliability risk*
Change Management Logs	Change requests, approvals, outcomes	Frequent rollbacks, emergency changes → *governance/control risk*
Audit Logs	Control execution history	Missed controls, skipped steps → *compliance risk*
Vendor Performance Reports	SLA adherence, service availability	Supplier reliability, contract risk
System Metrics / Monitoring Tools	CPU usage, latency, uptime percentages	Trends signaling performance degradation
HR / Training Logs	Incident training completion rates	Weak risk culture or awareness gaps

TECHNIQUES FOR ANALYSIS



Technique	Description	Example Application
Trend Analysis	Compare event frequency/severity over time	Monitor monthly incident count to detect growth trend
Baseline Comparison	Establish normal operating metrics and detect deviations	CPU load typically <60%; spike to 95% signals resource risk
Exception Filtering	Use queries to isolate outliers or unauthorized actions	Extract login attempts outside business hours
Correlation / Cross-Source Analysis	Combine multiple logs to uncover systemic patterns	Match network logs with help-desk tickets to locate root causes
Heat Mapping	Visualize risk occurrence by business unit, system, or time	Identify which process area contributes most to incidents
Root Cause Tagging	Label recurring errors by underlying process	Frequent deployment failures → inadequate QA or testing risk

LOG AND DATA REVIEW

- Deliverables and outputs
  - List of risk conditions identified
  - Example entries:
    - Increase in failed logins suggest possible credential abuse risk
    - Frequent unplanned system changes suggest inadequate change governance
    - Incident tickets recurring for same issue suggest ineffective corrective control
  - Preliminary risk statements
    - Condition → Event → Consequence format:
    - “If configuration changes are not reviewed (condition), systems may be deployed insecurely (event), resulting in data exposure (consequence)”
  - Summary dashboard or table
    - Columns: Data Source | Observation | Risk Category | Suggested Owner | Supporting Evidence
  - Cross-reference map
    - Align identified risks to controls, vulnerabilities, and assets: key ISACA practice for traceability

CHECKLISTS

- Checklists
  - Structured, repeatable tools used to identify known or foreseeable risks
  - Provide discipline, consistency, and traceability to the risk discovery process
  - Ensure that essential categories, controls, and scenarios are not overlooked
- Can be aligned with industry frameworks
  - ISACA, ISO 31000, NIST, DRI
  - Allow analysts to connect organizational practices to globally recognized standards
  - Provide a systematic method for scanning known risk areas and verifying that expected controls and practices exist
  - Complements the qualitative and data-driven methods (interviews, logs) by enforcing coverage and repeatability

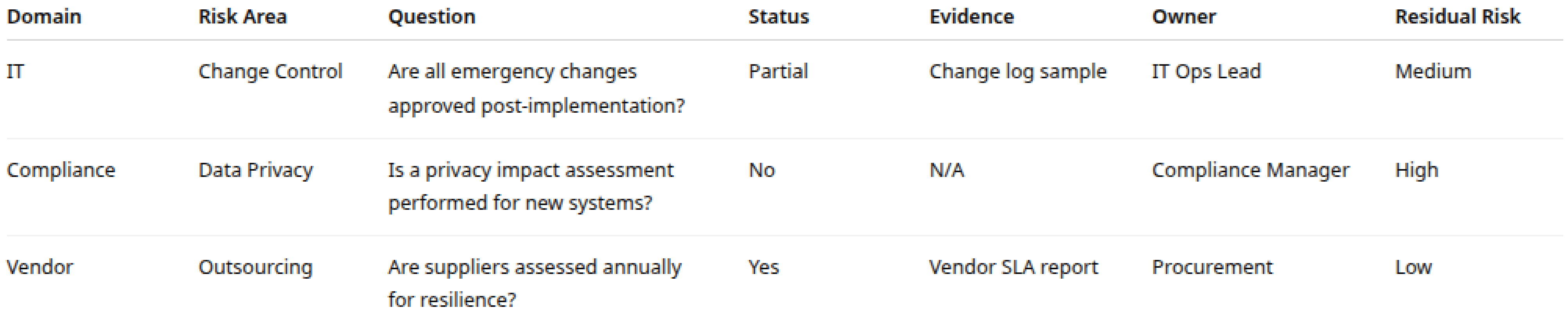
CHECKLISTS

- Value to analysts
  - Prevents risk “blind spots” by ensuring that all domains, systems, and process categories are reviewed
  - Translates abstract risk concepts into operationally testable questions
  - Supports audits, regulatory reviews, and resilience maturity assessments
- Relevance to risk typologies:
  - *Operational risks:* verify procedures, escalation, continuity
  - *Compliance risks:* ensure mandatory policies, records, or training exist
  - *Process and product risks:* confirm quality control, testing, and approval mechanisms
  - *Business/legal risks:* ensure contracts, third-party agreements, or insurance coverage align with appetite

CHECKLISTS

- Framework sources for checklist design
  - Purpose: Anchor checklist questions in recognized governance frameworks and resilience standards
- Building an effective risk checklist
  - Key components:
    - Risk domain headers: Operational, Financial, Strategic, Compliance, IT, HR, Vendor.
    - Question / test statement: “Are vendor performance reviews conducted at least quarterly?”
    - Expected evidence: Policy, report, log, or statement verifying existence
    - Status or rating field: “Yes / No / Partially Implemented”
    - Risk level or impact: High/Medium/Low or numeric scoring
    - Owner / reviewer: Accountability assignment

SAMPLE FORMAT (SPREADSHEET EXAMPLE)

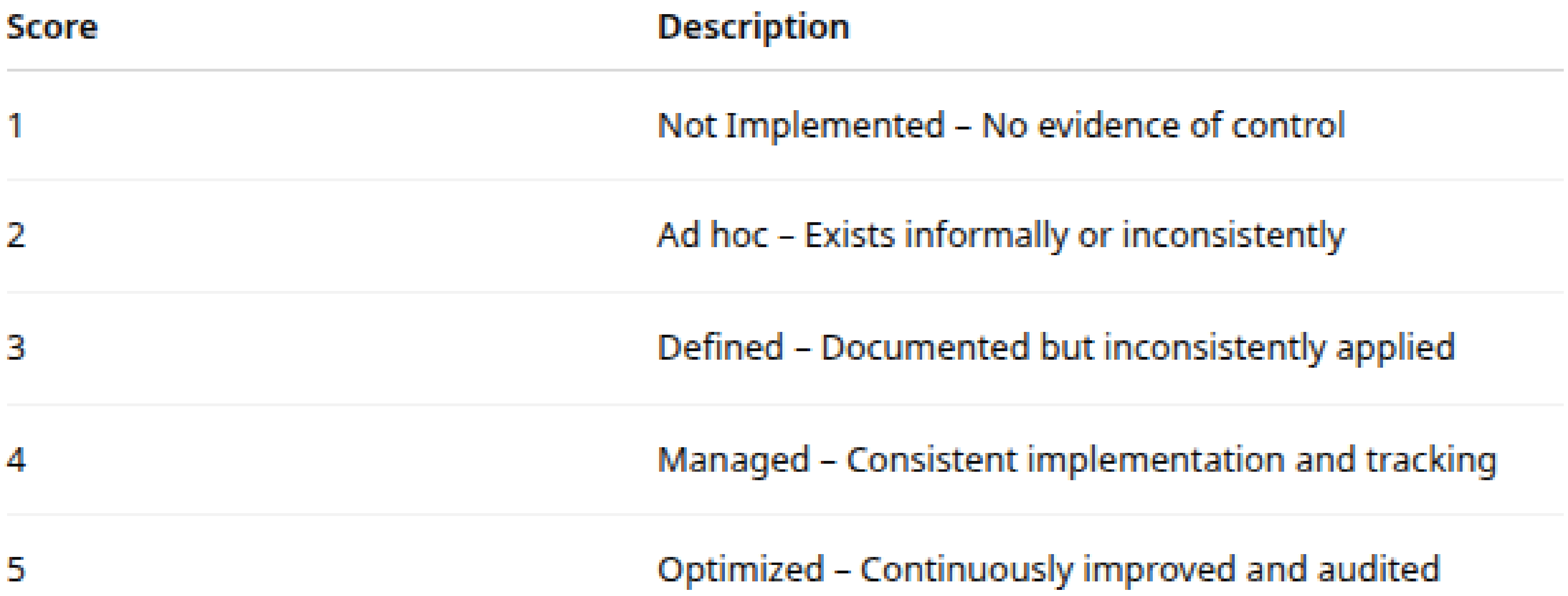


Domain	Risk Area	Question	Status	Evidence	Owner	Residual Risk
IT	Change Control	Are all emergency changes approved post-implementation?	Partial	Change log sample	IT Ops Lead	Medium
Compliance	Data Privacy	Is a privacy impact assessment performed for new systems?	No	N/A	Compliance Manager	High
Vendor	Outsourcing	Are suppliers assessed annually for resilience?	Yes	Vendor SLA report	Procurement	Low

CHECKLISTS

- Execution and scoring
  - Steps:
    - *Preparation*: Define scope (process, system, function)
    - *Apply checklist questions:* Through interviews, documentation review, or observation
    - *Record results:* Use Yes/No/Partial or maturity scores (1–5 scale)
    - *Summarize gaps:* Identify which controls or processes are missing or weak
    - *Rate associated risks:* Evaluate likelihood/impact of gaps and update the risk register

SCORING MODEL EXAMPLE



Score	Description
1	Not Implemented – No evidence of control
2	Ad hoc – Exists informally or inconsistently
3	Defined – Documented but inconsistently applied
4	Managed – Consistent implementation and tracking
5	Optimized – Continuously improved and audited

ADVANTAGES AND LIMITATIONS

- Advantages
  - Efficient, fast, and repeatable
  - Ideal for structured assessments, internal audits, and onboarding new analysts
  - Encourages organizational learning and forms a knowledge base for recurring assessments
  - Helps verify compliance and readiness for regulatory revie Evaluate likelihood/impact of gaps and update the risk register

ADVANTAGES AND LIMITATIONS

- Limitations
  - Focused on known risks: may miss new, emergent, or cultural risks
  - Over-reliance can promote “check-the-box” behavior
  - May not uncover systemic interdependencies (which require exploratory methods)
  - Requires periodic updates to remain relevant

BEST PRACTICES

- Completeness over creativity
  - Checklists ensure all baseline risk areas are covered, preventing oversight
- Framework traceability
  - Linking questions to standards (COBIT, ISO) enhances audit defensibility
- Periodic review
  - Checklist questions should evolve with changes in risk appetite, business models, or regulation
- Balance of depth vs breadth
  - Avoid excessively granular checklists that reduce focus; prioritize critical controls.
- Data validation
  - Combine checklist results with logs and interviews for a 360° view.

BEST PRACTICES

- Completeness over creativity
  - Checklists ensure all baseline risk areas are covered, preventing oversight
- Framework traceability
  - Linking questions to standards (COBIT, ISO) enhances audit defensibility
- Periodic review
  - Checklist questions should evolve with changes in risk appetite, business models, or regulation
- Balance of depth vs breadth
  - Avoid excessively granular checklists that reduce focus; prioritize critical controls.
- Data validation
  - Combine checklist results with logs and interviews for a 360° view.

EXPLORATORY RISK ANALYSIS

- Deep, open-ended investigation beyond checklists and standard models
  - Moves beyond compliance-driven reviews to learning-oriented inquiry
  - Encourages hypothesis-driven analysis (“What if this fails?”)
  - Supports DRI’s Prepare → Respond → Recover → Adapt lifecycle
  - Enables anticipation of systemic and cascading failures

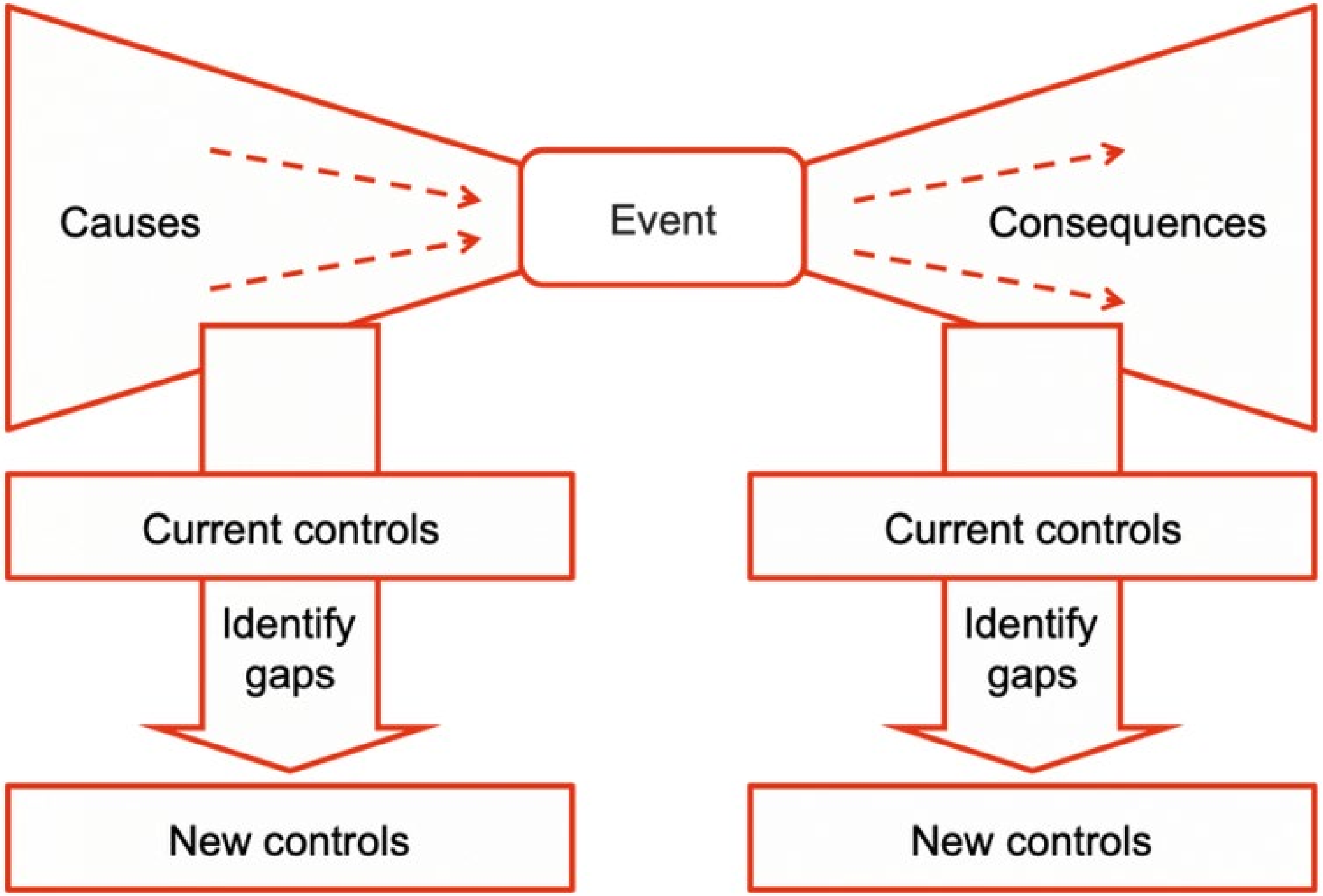
TECHNIQUES

- Scenario building and stress testing
    - Construct “What-if” scenarios around disruptions
        - For example: data center outage, insider threats
    - Assess second-order effects
        - For example: impacts on customers, supply chain, or reputation
    - Use qualitative scoring or Monte Carlo simulation for likelihood/impact analysis
    - Example: “What if the primary payment API fails on a Friday at month-end?”

TECHNIQUES

- Failure mode and effects analysis (FMEA)
  - Identify each process step’s potential failure modes, causes, and effect
  - Assign severity, likelihood, and detectability scores (S × L × D)
  - Prioritize high-risk failure points for mitigation
- Bow-Tie analysis
  - Visual model linking causes → event → consequences with corresponding controls
  - Helps visualize preventive and corrective control effectiveness

BOW TIE


Causes
Event
Consequences
Current controls
Current controls
Identify gaps
Identify gaps
New controls
New controls

TECHNIQUES

- Red team / tabletop exercises
  - Simulate adversarial or crisis conditions to test detection and response
  - Focus on cross-functional communication and control execution
- Trend and external signal scanning
  - Monitor emerging risk drivers: geopolitical, regulatory, technological
  - Use threat intelligence, audit findings, and industry reports to enrich risk awareness

ANALYSIS

- Cognitive and behavioral aspects
  - Avoid cognitive bias in assessment
    - Availability bias (overweighting recent incidents)
    - Groupthink (suppression of dissenting views)
    - Confirmation bias (seeking evidence to support existing beliefs)
  - Encourage diverse participation (operations, compliance, cyber, HR, vendors)

INTEGRATING EXPLORATORY RESULTS

- Translate findings into
  - New risk statements or control recommendations
  - Lessons learned feeding into SOPs, training, and testing cycles
- Correlate exploratory insights with risk appetite and tolerance thresholds
  - High-impact, low-probability events → evaluate residual risk vs. risk capacity
- Example:
  - A ransomware simulation reveals that supplier data access is unmonitored
  - Results in new risk category: third-party data exposure

OUTPUT AND GOVERNANCE

- Document outcomes in risk workshop reports, including
  - Discovered risks, assumptions, unknowns, early warning indicators
  - Mitigation proposals and ownership
- Feed results into risk registers and resilience improvement plans

Q&A AND OPEN DISCUSSION