RISK AND RESILIENCE BOOTCAMP

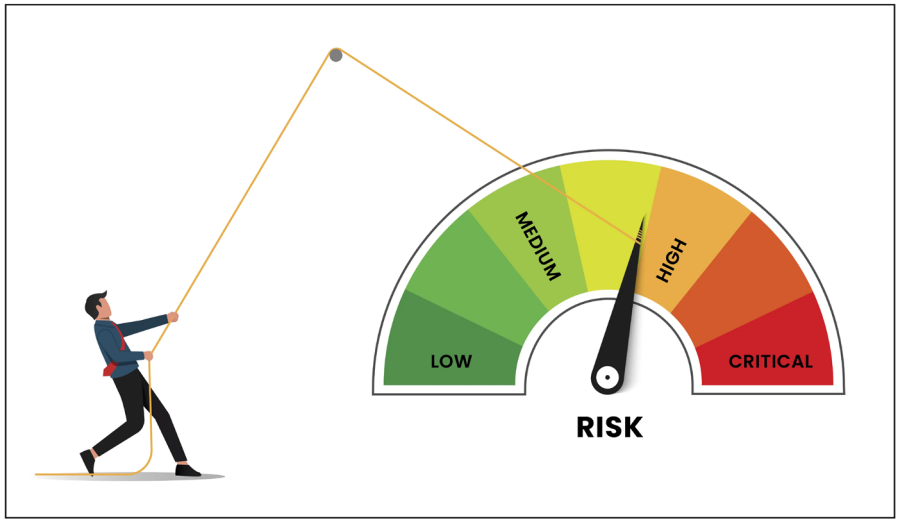
TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK INDICATORS AND MONITORING

This module is an introduction to risk indicators and risk monitoring

- Key Risk Indicators
- Key Performance Indicators
- Risk Monitoring Methods



KPI AND KRI FUNDAMENTALS

- In mature risk and operations environments
  - KPIs and KRIs support a resilient organization
    - Enable monitoring of system health
    - Anticipate emerging risks
    - Align operational performance with strategic risk appetite
  - KPIs reflect how well controls and processes are functioning
  - KRIs indicate how monitors thresholds where risk materializes as incidents
  - Together, they enable predictive risk management

KEY PERFORMANCE INDICATORS

- KPIs are performance metrics
  - Quantify the effectiveness, efficiency, and reliability of IT processes, teams, and technologies
  - Measure how well the organization is executing its operational duties and whether its control environment is functioning as intended
  - KRIs reveal risk exposure while KPIs measure operational maturity
- Properties of high quality KPIs
  - Leading and lagging
  - Context specific
  - Aligned to critical services
  - Traceable to controls

LEADING INDICATORS

- Leading indicators predict what is about to happen
  - Provide early warnings of potential risk or performance degradation before an incident or failure occurs
    - They are precursors or signs that risk exposure is increasing
  - Characteristics
    - Predictive
    - Forward-looking
    - Based on behaviors, conditions, or patterns that precede an outcome
    - Used to anticipate issues and take preventative action

LEADING INDICATORS

- Leading indicators predict what is about to happen
  - Examples
    - Increasing number of failed login attempts (predicts account compromise)
    - Rising backlog of unpatched vulnerabilities (predicts future breach likelihood)
    - Sudden spike in CPU saturation events (predicts upcoming service outage)
    - Growing number of “near miss” incidents (predicts operational fragility)
    - Increasing time required to complete daily backups (predicts future backup failures)

LAGGING INDICATORS

- Measure events after they have occurred.
  - They record how the organization performs historically
    - Describe what has happened, not what is about to happen
  - Characteristics
    - Retrospective
    - Outcome-based
    - Concrete evidence of success or failure
    - Useful for evaluating control effectiveness and operational maturity
  - Examples
    - Number of security incidents last quarter
    - Mean Time to Recover (MTTR) from outages
    - Change failure rate in production
    - % of critical vulnerabilities successfully remediated
    - Amount of data loss from an incident

LEADING AND LAGGING INDICATORS

- A mature KPI/KRI framework includes both types because
  - Leading indicators help prevent incidents
    - They enable proactive risk management
  - Lagging indicators measure the impact of incidents and performance
    - They validate whether controls, teams, and processes actually worked
- Analogy
  - Leading = smoke detector
    - “Something bad is likely to happen soon.”
  - Lagging = fire damage report
    - “This is what happened, and how badly.”

LEADING AND LAGGING INDICATORS

- Example: patch management
  - Leading
    - Count of unpatched critical vulnerabilities which predicts elevated cyber risk
  - Lagging
    - Number of systems compromised due to unpatched software which measures the realized impact
- Example: service reliability
  - Leading
    - Increase in average CPU load & latency deviation which predicts upcoming service outage
  - Lagging
    - MTTR for last outage which measures how effectively the team recovered

CONTEXT-SPECIFIC INDICATORS

- KPIs and KRIs must be context-specific
  - Intentionally designed to fit the unique characteristics of the organization's environment
  - A metric that is highly meaningful in one enterprise can be irrelevant or misleading in another
  - To be context-specific, indicators must reflect
    - The organization's technology stack
    - The regulatory and compliance environment
    - The operational and risk maturity level
  - Only when KPIs/KRIs are aligned to these dimensions do accurately measure performance, signal risk exposure, and support effective decision-making

CONTEXT-SPECIFIC INDICATORS

- IT environments have
  - Distinct IT architectures
  - Unique toolchains for development and deployment
  - Specific integration patterns and system dependencies
  - Metrics must reflect the actual systems in place to provide useful insights
- Concerns
  - Metrics that assume cloud-native architecture are meaningless in a mainframe-centric environment
  - Vulnerability KRIs differ significantly between containerized microservices and legacy monolithic applications
  - DevOps KPIs like deployment frequency are irrelevant when CI/CD pipelines are not used

CONTEXT-SPECIFIC INDICATORS

- Examples
  - Cloud-native environments
    - KRI: Number of misconfigured IAM roles
    - KPI: Mean time to detect drift from Infrastructure-as-Code baselines
  - Legacy environments
    - KRI: Number of unsupported OS instances
    - KPI: Batch job completion success rate
  - Microservices / Kubernetes
    - KRI: Pod restart frequency as an indicator of underlying instability
    - KPI: Service mesh policy enforcement rate
  - SaaS-heavy environments
    - KRI: Third-party vendor incident notifications per quarter
    - KPI: Integration error rates (API failures)

CONTEXT-SPECIFIC INDICATORS

- Regulatory environment
  - Every industry faces unique compliance obligations
  - Metrics reflect the external compliance standards criteria of acceptable risk levels
    - Financial institutions must track KRIs related to operational resilience, fraud, and audit failures
    - Healthcare organizations must monitor privacy, data integrity, and change control fidelity
    - Global enterprises operating in multiple jurisdictions encounter a collection of requirements
- Examples
  - Banking / Financial Services
    - KRI: Number of untested business continuity plans
    - KPI: Timeliness of required regulatory reports such as suspicious activity reports

CONTEXT-SPECIFIC INDICATORS

- Examples
  - Healthcare
    - KRI: Privacy breach near misses / PHI exposure attempts.
    - KPI: % of access logs reviewed within mandated time windows (HIPAA)
  - Critical Infrastructure / Energy
    - KRI: Number of NERC Critical Infrastructure Protection control deviations
    - KPI: Patch deadline adherence for ICS/SCADA systems
- Regulatory context determines
  - Which metrics matter
  - Thresholds for escalation
  - Acceptable levels of residual risk

CONTEXT-SPECIFIC INDICATORS

- Organizational Maturity
  - Different stages of risk maturity require metrics that match their capabilities and governance levels
  - Metrics that are too advanced for a low-maturity environment will not be reliably collected, interpreted, or acted on
  - Overly simplistic metrics cannot guide a high-maturity organization

CONTEXT-SPECIFIC INDICATORS

- Low maturity (reactive operations)
  - Primary focus: visibility and correctness of basic processes
  - KPIs:
    - % incidents with a documented root cause
    - Change success rate
  - KRIs:
    - Unreviewed production changes
    - Number of unauthorized access attempts
  - Purpose: establish foundational hygiene

CONTEXT-SPECIFIC INDICATORS

- Mid maturity (stable, repeatable processes)
  - Primary focus: operational consistency and trend monitoring
  - KPIs:
    - Automated test coverage in CI/CD pipelines
    - MTTD/MTTR for major incidents
  - KRIs:
    - Increasing trend in “near misses”
    - Technical debt growth rate
  - Purpose: strengthen resilience and detect leading risk indicators

CONTEXT-SPECIFIC INDICATORS

- High maturity (data-driven, predictive operations)
  - Primary focus: predictive analytics, optimization, and strategic alignment
  - KPIs:
    - Policy-as-code enforcement rate
    - Ratio of autonomous vs. manual remediation actions
  - KRIs:
    - Threat landscape deviation index (AI-based risk analytics)
    - Probability-weighted operational risk forecast metrics
  - Purpose: enable proactive, adaptive risk management informed by real-time intelligence

KPI CATEGORIES

- Process effectiveness KPIs
  - Change success rate
  - % of incidents resolved within SLA
  - Release rollback frequency
- Operational reliability KPIs
  - Uptime/availability percentages
  - Backup job success rates and restore success rates
  - Configuration drift frequency
- Security operations KPIs
  - Mean Time to Detect (MTTD)
  - Mean Time to Respond (MTTR)
  - SFalse-positive and false-negative rates in SIEM alerts

KPI CATEGORIES

- Control-maturity KPIs
  - Patch compliance rate
  - Privilege access review completion rate
- Automation and efficiency KPIs
  - Ratios of automated vs. manual remediations
  - Time-to-deploy infrastructure changes (CI/CD velocity)

KPI CATEGORIES AND RISK

- KPIs have indirect risk implications:
  - Rising MTTR → control or resource gaps → elevated operational risk
  - Low change success rate → increased likelihood of incidents → resilience degradation
  - Backup failures → increased data loss risk → potential compliance violations
  - KPIs are essential for correlating control performance with risk posture

KEY RISK INDICATORS

- Measure conditions that signal increasing probability or impact of a risk event
  - KPIs measure health, KRIs measure fragility
  - KRIs are fundamentally predictive
  - Aim to detect early deviations that failures of some type
- High quality KRIs
  - *Forward looking*: Detect emerging risks before they materialize
  - *Threshold driven:* Have defined trigger levels for escalation (green/yellow/red)
  - *Statistically grounded*: Derived from trend analysis, control effectiveness data, and risk scenarios
  - *Automated*: Generated from SIEM, SOAR, cloud dashboards, or GRC platforms
  - *Mapped to risk appetite*: Tied directly to organizational tolerance limits

KEY RISK INDICATORS

- KRI categories
  - Security exposure KRIs
    - Volume of unpatched critical vulnerabilities
    - Failed login attempt ratios (high → brute-force or credential-stuffing risk)
    - Rate of privilege escalation requests
  - Operational fragility KRIs
    - % of infrastructure approaching end-of-life
    - Incidence of repeated near-misses
    - Unplanned configuration changes (indicator of change process breakdown)
  - Resilience and availability KRIs
    - Frequency of system saturation events (CPU, memory, IOPS)
    - Latency deviation from baseline in critical services
    - Growth rate of technical debt backlog

KEY RISK INDICATORS

- KRI categories
  - Cloud risk KRIs
    - Misconfigured IAM roles detected
    - Number of public-facing S3 buckets or exposed services
    - Drift from baseline security posture in cloud cloud security posture management scans
  - Compliance KRIs
    - Exception count in critical controls
    - Number of overdue regulatory tasks
    - Third-party systems and organizational controls report exceptions
- KRIs
  - Signal that a system, process, or control environment is approaching a risk threshold.
  - Answer the question “How close are we to a risk event?”

KPI AND KRI MATURITY

- In high-maturity organizations
  - KPIs and KRIs are not passive, descriptive metrics living in static dashboards
  - They are part of a dynamic, intelligence-driven ecosystem
  - Supports operational resilience, risk-informed decision-making, and strategic governance
  - Integrate with automation pipelines, cyber-defense mechanisms, resilience engineering, and board-level reporting

KPI AND KRI MATURITY

- Integrated risk and performance analytics
  - KPIs and KRIs are not interpreted in isolation
  - They are analyzed together to system-wide risk patterns (systems analysis)
  - Integration insights
    - A KPI may appear healthy even as the associated KRIs show escalating exposure
    - A deteriorating KPI can reveal structural weaknesses that elevate KRIs downstream
    - Combined analysis uncovers feedback loops, interdependencies, and hidden systemic risks
- Analytical techniques
  - Correlation analysis
    - Identifies statistical relationships between operational performance and risk exposure
    - Example: Increased change failure rate often correlates with rising incident frequency

KPI AND KRI MATURITY

- Analytical techniques
  - Causal pathway mapping
    - Used to identify whether one metric drives another
    - Example: Patch latency → rising vulnerability count → higher breach likelihood
  - Multivariate analysis
    - Multiple KPIs/KRIs analyzed simultaneously to identify clusters of weak signals
  - Systemic trend analysis
    - Viewing metrics across applications, business units, or regions to detect enterprise-wide weaknesses
- Integrated analytics enable
  - Earlier detection of complex or cascading risks
  - More accurate root cause analysis
  - A unified view for executive decision-making

DYNAMIC THRESHOLDING

- Dynamic thresholding
  - Static thresholds (e.g., “alert if CPU > 80%”) are insufficient in modern environments
  - Thresholds must adjust to context, behavior, and historical patterns
  - driven by cloud elasticity, microservices, rapid deployment rates, and dynamic threat environments
- Techniques
  - Baseline modeling
    - Establishes “normal” operational behavior for a system
    - Baselines adapt as the system evolves
    - Example: Network throughput baseline for a trading platform might double during seasonal market activity

DYNAMIC THRESHOLDING

- Techniques
  - Anomaly detection
    - Modern monitoring platforms integrate statistical and ML techniques:
    - Z-score modeling to detect outliers
    - Clustering algorithms (e.g., DBSCAN) to find unusual patterns
    - Machine learning models to learn normal behavior and flag deviations
  - These detect
    - Sudden spikes in authentication failures
    - Unexpected changes in deployment frequency
    - Anomalous outbound traffic (possible exfiltration)

DYNAMIC THRESHOLDING

- Techniques
  - Seasonality adjustments
  - Some behaviors recur predictably:
    - Payroll spikes
    - Holiday e-commerce surges
    - Backup system load at month-end
  - Advanced systems incorporate seasonality into threshold calculations to reduce false positives
- Dynamic thresholding:
  - Decreases noise
  - Increases sensitivity to real risk events
  - Enables context-aware alerting

PREDICTIVE RISK FORECASTING

- KRIs evolve
  - From descriptive measurements to predictive tools for future-state risk modeling
  - This is characteristic of high-maturity ERM and cyber-resilience programs
- Predictive analytics
  - KRIs feed into machine learning models that forecast
    - Outage probabilities
    - Security incident likelihood
    - Control failure trends
    - Capacity risk
  - These forecasts leverage historical data and real-time telemetry

PREDICTIVE RISK FORECASTING

- Risk heatmaps (dynamic)
  - Instead of static matrices, advanced heatmaps update
    - Automatically
    - Continuously
    - With probabilistic scoring
  - Incorporating both current and forecasted risk ratings
- Scenario simulations
  - Organizations run “what-if” simulations
    - What if patch latency increases by 40%?
    - What if credential stuffing attacks triple next month?
    - What if cloud costs force reduction in redundancy?

PREDICTIVE RISK FORECASTING

- Monte Carlo analysis
  - Used in financial risk, but increasingly in cyber operations:
  - Runs thousands of simulated futures
  - Produces probability distributions of loss events
  - Helps quantify tail-risk exposure
- Predictive forecasting supports
  - Board-level conversations
  - Budget prioritization
  - Investment in resilience programs
  - Regulatory reporting, especially operational resilience mandates

CONTROL EFFECTIVENESS FEEDBACK LOOPS

- How the feedback loop works example
  - Step 1: Mapping KRIs to controls
    - KRI: Number of misconfigured cloud storage buckets
    - Maps to: NIST PR.AC-4 (Access Management) & CIS 3.11 (Secure Configurations)
  - Step 2: Threshold reach
    - A KRI exceeds tolerance
    - Misconfigured buckets increase from 3 to 27 in one quarter
  - Step 3: Reassessing control effectiveness
    - Are existing controls insufficient?
    - Have processes degraded?
    - Has system complexity increased?
    - Are new attack vectors emerging?

CONTROL EFFECTIVENESS FEEDBACK LOOPS

- How the feedback loop works example
  - Step 4: Triggering Remediation
  - Approach depends on severity of risk, for example for a authentication risk
  - Compensating controls
    - Additional IAM monitoring
    - Temporary manual review processes
  - Immediate remediation
    - Automated enforcement of configuration baselines
    - Access revocations
  - Reprioritizing risk programs
    - Invest in cloud security posture management (CSPM)
    - Update policies
    - Provide specialized training

CONTROL EFFECTIVENESS FEEDBACK LOOPS

- How the feedback loop works example
  - Step 5: Closing the loop
    - Re-measure KRI after remediation
    - Update thresholds or metrics if necessary
    - Feed insights back into governance committees
- Control environments evolve dynamically, ensuring resilience as technology and threats change

RESILIENCE ENGINEERING

- Focuses on ensuring systems continue to operate under stress, failure, or adversity
  - Mature organizations leverage KRIs to actively inform resilience strategy
- How KRIs support resilience
  - Predicting resource saturation by identifying
    - CPU saturation patterns
    - Memory leaks
    - Latency degradation
    - IOPS constraints
  - Feed into forecasting tools that signal when:
    - Auto-scaling thresholds need adjusting
    - Additional capacity planning is required

RESILIENCE ENGINEERING

- How KRIs support resilience
  - Revealing single points of failure by measuring
    - Repeated service restarts
    - Redundancy failures
    - VPN gateway overload
  - Providing data for BC/DR decisions using
    - RTO/RPO recalibration
    - Alternate site failover decisions
    - Data replication strategies

RESILIENCE ENGINEERING

- How KRIs support resilience
  - Triggering architectural rework by showing chronic issues suggesting
    - Service decomposition
    - Database sharding
    - Network segmentation
    - Cloud region diversification
  - Enabling adaptive response in dynamic environment
    - Integrate with Security Orchestration, Automation, and Response platforms
    - Behavior deviations trigger automated corrective actions
    - The system “self-heals” where possible
- Organizations shift from reactive recovery to anticipatory resilience, reducing incident frequency and impact

MONITORING KRIS

- Monitoring KRIs is not simply setting up a dashboard
  - KRI monitoring is built onData pipelines
    - Defined thresholds
    - Alerting logic
    - Governance workflows
    - Regular review cycles.
- Typically includes six operational components

MONITORING KRIS

- 1. Telemetry collection from data sources
  - Security Information and Event Management (SIEM) tools (Splunk, Sentinel, QRadar)
  - Cloud security posture tools (AWS Security Hub, Azure Defender, GCP SCC)
  - Cloud security posture management, Cloud workload protection platforms
  - Identity systems (Okta, Azure AD, CyberArk)
  - Endpoint detection platforms (CrowdStrike, SentinelOne)
  - CI/CD pipelines (GitLab CI, Jenkins, GitHub Actions)
  - Incident management platforms (ServiceNow, PagerDuty)
  - Vulnerability scanners (Tenable, Qualys, Rapid7)
  - Network monitoring tools (Datadog, Prometheus, NetFlow)
  - GRC systems (MetricStream, Archer, ServiceNow GRC)

MONITORING KRIS

- 2. KRI calculations from operational metrics
  - Raw data is ingested and processed into quantified KRI values
    - Counts (e.g., # of privileged access exceptions)
    - Ratios (e.g., failed/successful login attempts)
    - Rates (e.g., patching latency growth rate)
    - Scores (e.g., vulnerability severity index)
    - Forecasts (e.g., projected capacity saturation in 60 days)
  - Calculations may be
    - Real-time
    - Batch (hourly, daily)
    - Triggered by events (e.g., access approval workflow)

MONITORING KRIS

- 3. Threshold Management
    - KRIs require thresholds tied to risk appetite such as
  - Static thresholds
    - Example: “# of critical vulnerabilities > 200 triggers escalation.”
  - Dynamic thresholds
    - Based on baseline behavior (machine learning, moving averages)
    - Example: “Alert if failed logins exceed baseline by 3 standard deviations.”
  - Regulatory thresholds
    - Example: “Any unencrypted PHI transmission = immediate escalation” (HIPAA).
    - Thresholds must be reviewed regularly by Risk Committees.

MONITORING KRIS

- 4. Alerting and escalation paths
  - When a threshold is breached, monitoring systems trigger
    - SIEM alerts
    - Real time notifications to incident response teams
    - Creation of incident records
    - Governance, Risk, and Compliance (GRC) workflow escalations
    - Automated Slack/Teams messages
  - Escalation tiers are based on severity and potential business impact

MONITORING KRIS

- 5. Governance and Human Review
  - KRI results feed into
    - Daily standups for operational teams
    - Weekly operational risk committee reviews
    - Monthly CISO/CRO briefings
    - Quarterly board-level risk reports
    - Annual regulatory audits
  - Some KRI categories (e.g., high vulnerability counts) trigger mandatory reporting in many regulated industries

MONITORING KRIS

- 6. Feedback Into Controls and Mitigation
  - KRI breaches often lead to control reassessment
    - Are preventive controls failing?
    - Do detective controls need tuning?
    - Do we need a compensating control?
    - Should this drive a new mitigation project?
  - High-maturity organizations run this as a closed feedback loop.

CYBERSECURITY KRIS

- Volume of unpatched critical vulnerabilities
  - Why it matters
    - Directly linked to breach likelihood
  - How it's monitored
    - Vulnerability scanners (Qualys, Tenable) feed daily reports into a central SIEM
    - Scanners categorize by CVSS score, asset criticality, exploit availability
  - Threshold examples
    - Green: < 50 high/critical vulnerabilities
    - Yellow: 50–200
    - Red: > 200 (triggers CISO-level escalation)
  - Action
    - Automated ticket creation for asset owners
    - Prioritize patching based on exploitability
    - Escalate overdue remediation cases to governance

OPERATIONAL RESILIENCE KRIS

- Increase in “Near Miss” operational incidents
  - How it’s monitored
    - ServiceNow incident tickets tagged as “near misses”
    - Trend analysis run monthly
  - Why it matters
    - Near misses statistically precede major incidents
  - Action
    - Root cause analysis workshops
    - Process redesign

IDENTITY AND ACCESS KRIS

- Number of Stale Accounts (Dormant > 90 days)
  - How it’s monitored
    - Identity governance tools identify unused accounts
    - High-risk because attackers exploit dormant accounts
  - Action
    - Automated cleanup workflow
    - Quarterly reviews mandated by policy

HIGH-MATURITY MONITORING

- Organizations with mature KRI monitoring have:
  - Automated log ingestion and KRI computation
  - Dynamic thresholds based on machine learning
  - Unified dashboards integrating KPIs, KRIs, and business impacts
  - Board-level reporting with forward-looking KRI forecasts
  - Tight integration with SOAR, GRC, and ITSM systems
    - SOAR = Security Orchestration, Automation, and Response
    - GRC = Governance, Risk, and Compliance
    - ITSM = IT Service Management
  - Strong feedback loops into control optimization

Q&A AND OPEN DISCUSSION