

RISK AND RESILIENCE BOOTCAMP





RISK MAPPING

This module looks at the process of risk mapping

- Identifying specific resources, people and processes where identified risk can occur
- Assessment of the real world vulnerabilities that can be exploited by a risk event



RISK MAPPING

- Process of
 - Identifying visualizing and prioritizing operational risks across systems, processes, and technologies
- Provides structured view of
 - Vulnerabilities exist within IT operations
 - How failures or threats in those areas could impact business continuity or service availability
- From a resilience perspective, risk mapping helps operations teams:
 - Understand where key failure points exist
 - Prioritize controls and monitoring
 - Align mitigation plans with business-critical assets
 - Support decision-making for resource allocation and automation
- Turns abstract risk discussions into actionable visual and process-based plans

RISK MAPPING

- Operational environments are complicated
 - Combinations of on-premises, hybrid, or cloud
 - Complex ecosystems involving
 - Infrastructure, software, people, and third-party dependencies
 - Without a clear risk map, responds tend to be reactive instead of proactive
- Role of a risk map
 - Links technology components (servers, APIs, networks) to business services
 - Shows dependencies and cascading failure points
 - Highlights where controls are applied or missing
 - Enables resilience-by-design through targeted process improvements

RISK MAPPING

- Building a risk map
 - Identify operational domains
 - List all critical systems and services: compute, network, storage, identity, monitoring, etc
 - List key activities and dependencies
 - For each system, document operational processes
 - For example: patching, user access, backup
 - Assess risks and controls
 - Identify where failures could occur and the current controls in place
 - Assign risk ratings
 - Use a simple risk scoring model to assign risk
 - Visualize
 - Use a heat map or matrix to display risk levels across processes and technologies
 - Looking for potential points of failure or vulnerabilities to threat
 - Prioritize actions
 - Direct resources toward the highest residual risks, those least controlled

RISK MAPPING

- Integration with SOPs and continuous improvement
 - Risk mapping is not a one-time exercise, it is an ongoing process
 - Feeds into
 - Continuous monitoring dashboards
 - Post-incident reviews and corrective action plans
 - SOP updates and process reviews
 - Training for operational teams to raise awareness of risk ownership.
- Mature risk and resilience program uses risk mapping to
 - Continuously align operational practices with business priorities
 - Detect weak points before failure
 - Validate recovery capability through testing and measurement

EXAMPLE

- Risk Mapping for IT Operations
 - Web-based banking application hosted in a hybrid cloud environment.
 - Operations include patching, access management, backup, monitoring, and incident response
 - The goal of the risk map is to identify where failures or vulnerabilities may occur and how well existing controls protect against them.
 - Step 1: Identify key operational domains
 - Patching OS and application updates
 - Access Control User and admin account management
 - Backup Data protection and recovery
 - Monitoring System and service health checks
 - Incident Response Issue triage and communication

EXAMPLE

- Step 2: Identify risks, likelihood, and impact

Domain	Example Risk	Likelihood	Impact	Initial Risk Level
Patching	Missed security patch leads to exploit	Medium	High	High
Access	Former employee retains access	Low	High	Medium
Backup	Backup copy corrupted	Low	High	Medium
Monitoring	Critical alert missed due to misconfiguration	Medium	Medium	Medium
Incident Response	Delayed escalation during outage	Medium	High	High

EXAMPLE

- Step 3: Identify controls

Domain	Control Implemented	Control Type	Control Maturity	Residual Risk
Patching	Automated patch management with testing	Preventive	Medium	Medium
Access	Role-based access and MFA	Preventive	High	Low
Backup	Weekly restore tests; offsite copy	Corrective	Medium	Low
Monitoring	Centralized alerts with escalation	Detective	Medium	Medium
Incident Response	SOPs and on-call schedule	Corrective	Low	Low

EXAMPLE

- Step 4: Visualize as a risk heat map

Impact ↓ / Likelihood →	Low	Medium	High
High Impact	Access (Low residual)	Patching, Incident Response (Medium residual)	—
Medium Impact	Backup (Low residual)	Monitoring (Medium residual)	—
Low Impact	—	—	—

EXAMPLE

- Step 5: Interpret the map
 - High-risk areas
 - Patching and Incident Response: need process improvement or stronger automation
 - Low-risk areas
 - Access and Backup: mature controls already in place
 - Next step:
 - Focus improvement on patch management automation and escalation response time

OPERATIONAL DOMAINS TO MAP

- Patching and vulnerability management
 - Maintain system integrity and security by keeping software current

Aspect	Typical Risks	Controls / Mitigations
Patch delays or skipped updates	Exposure to known vulnerabilities	Automated patch management tools, patch testing environments
Poor change management	Unplanned downtime or service disruption	Staged patch deployment, rollback plans
Incomplete inventory	Unpatched assets remain unnoticed	Asset discovery and configuration management databases (CMDBs)
Outdated third-party components	Compromised dependencies	Dependency scanning, vendor monitoring
Resiliency tie-in: Timely and controlled patching reduces attack surfaces and helps maintain stable, secure operations.		

OPERATIONAL DOMAINS TO MAP

- Access management
 - Ensure that only authorized individuals have the right level of access to systems and data

Aspect	Typical Risks	Controls / Mitigations
Excessive privileges	Insider threats, misuse	Role-based access control (RBAC), least privilege principle
Poor offboarding	Former employees retain access	Automated deprovisioning, periodic access reviews
Weak authentication	Credential theft or compromise	Multi-factor authentication (MFA), privileged access management (PAM)
Shared credentials	Accountability loss	Identity and Access Management (IAM) enforcement

Resiliency tie-in: Proper access management limits potential damage and speeds recovery by ensuring clear accountability and control boundaries.

OPERATIONAL DOMAINS TO MAP

- Backup and data protection
 - Preserve data availability and integrity in the event of system failure, corruption, or attack (e.g., ransomware)

Aspect	Typical Risks	Controls / Mitigations
Missing or outdated backups	Data loss	Automated, scheduled backups with monitoring
Inaccessible backups	Backup media corruption or offline storage	Regular restoration tests
Backup stored with production data	Ransomware encrypts both	Offsite or immutable (air-gapped) backups
No recovery validation	Backups fail during crisis	Periodic recovery drills, audit logs
Resiliency tie-in: Reliable backups enable rapid restoration and continuity, making recovery a managed process instead of a crisis response.		

OPERATIONAL DOMAINS TO MAP

- Monitoring and alerting
 - Detect anomalies, performance degradation, and failures early to enable fast response

Aspect	Typical Risks	Controls / Mitigations
Missing or outdated metrics	Blind spots in operations	Comprehensive instrumentation
Alert fatigue	Ignored critical warnings	Alert prioritization, correlation, and noise reduction
Monitoring tool outages	Delayed detection	Redundant monitoring, self-monitoring alerts
Lack of escalation	Slow incident response	Defined escalation paths, runbooks

Resiliency tie-in: Effective monitoring forms the **detective control backbone** of resilient operations.

OPERATIONAL DOMAINS TO MAP

- Incident and problem management
 - Detect anomalies, performance degradation, and failures early to enable fast response

Aspect	Typical Risks	Controls / Mitigations
Poor incident triage	Extended outages	Tiered response process and severity classification
Lack of root cause analysis	Repeat failures	Post-incident reviews and problem tracking
Incomplete documentation	Loss of institutional knowledge	Centralized incident tracking systems
Weak communication	Stakeholder confusion	Incident communication plans and templates

Resiliency tie-in: Incident management ensures **detective and corrective controls** function effectively, minimizing downtime.

OPERATIONAL DOMAINS TO MAP

- Capacity and performance management
 - Detect anomalies, performance degradation, and failures early to enable fast response

Aspect	Typical Risks	Controls / Mitigations
Resource saturation	Service slowdowns or crashes	Load testing, capacity forecasting
Over-provisioning	Wasted resources and cost inefficiency	Elastic scaling (cloud), monitoring
Ignoring growth trends	Unexpected capacity shortfall	Regular capacity reviews
Lack of visibility	Inability to plan scaling	Performance monitoring dashboards

Resiliency tie-in: Anticipating resource limits prevents service degradation and maintains user experience.

OPERATIONAL DOMAINS TO MAP

- Network and connectivity management
 - Maintain secure and reliable network connectivity between systems and users

Aspect	Typical Risks	Controls / Mitigations
Misconfigured firewalls	Connectivity failures or open exposure	Change-controlled firewall policies
Single points of failure	Network outages	Redundant links, failover routing
Unmonitored latency	Degraded service performance	Continuous network monitoring
Unauthorized access	Breach or lateral movement	Network segmentation, Zero Trust design

Resiliency tie-in: Network redundancy and monitoring ensure operations can continue despite link or device failures.

OPERATIONAL DOMAINS TO MAP

- Data integrity and database operations
 - Maintain accuracy, consistency, and recoverability of data across all systems

Aspect	Typical Risks	Controls / Mitigations
Corrupted or inconsistent data	Business impact, inaccurate reporting	Transaction integrity checks, replication verification
Poor backup discipline	Data loss	Point-in-time recovery, log archiving
Unauthorized queries or changes	Data breach	Database access control, auditing
Schema drift or version mismatch	Application errors	Controlled migrations, DevOps database pipelines

Resiliency tie-in: Ensures that business-critical data remains trustworthy and recoverable after an incident.

OPERATIONAL DOMAINS TO MAP

- Vendor and third-party dependency management
 - Manage risk from external suppliers, platforms, and service providers

Aspect	Typical Risks	Controls / Mitigations
Vendor outages	Service disruption	Multi-vendor redundancy, SLA monitoring
Data exposure via vendor	Compliance breach	Vendor risk assessments, contractual security clauses
Hidden dependencies	Unclear failure domains	Dependency mapping, SBOM tracking
Poor communication during incidents	Delayed recovery	Escalation contacts and periodic vendor reviews

Resiliency tie-in: Builds awareness of external dependencies and ensures continuity when third-party services fail.

OPERATIONAL DOMAINS TO MAP

- Change and release management
 - Manage updates, deployments, and system configuration changes without disrupting operations

Aspect	Typical Risks	Controls / Mitigations
Uncontrolled or untested changes	Production outages or regressions	Formal change control process, CAB approval
Lack of rollback plan	Extended downtime	Automated deployment scripts with rollback
Change schedule conflicts	Resource contention, downtime overlap	Integrated release calendar, change freeze periods
Insufficient communication	User or system impact	Notification and stakeholder coordination

Resiliency tie-in: Structured change management reduces unintended downtime and enables predictable recovery.

OPERATIONAL DOMAINS TO MAP

- Configuration management
 - Ensure systems and software are consistently and securely configured across environments

Aspect	Typical Risks	Controls / Mitigations
Configuration drift	Inconsistent behavior between systems	Configuration baselines, automated enforcement (Ansible, Puppet, Chef)
Unauthorized changes	Hidden vulnerabilities	Change monitoring, integrity verification
Lack of version control	Difficult rollback or audit	Configuration repositories and versioning
Weak documentation	Hard to rebuild or restore	CMDB with configuration records

Resiliency tie-in: Proper configuration management enables rapid re-creation of environments after failure or compromise.

OPERATIONAL DOMAINS TO MAP

- Logging and audit management
 - Maintain detailed, tamper-proof logs for forensics, compliance, and risk analysis

Aspect	Typical Risks	Controls / Mitigations
Missing or incomplete logs	Limited visibility during incidents	Centralized log aggregation
Log tampering	Undetected attacks	Immutable or signed logs
Log overload	Storage and analysis inefficiency	Log retention policies, filtering
No audit process	Missed compliance violations	Scheduled reviews, SIEM correlation rules

Resiliency tie-in: Reliable logging supports **detective and forensic recovery** after an event.

OPERATIONAL DOMAINS TO MAP

- Disaster recovery and business continuity
 - Maintain detailed, tamper-proof logs for forensics, compliance, and risk analysis

Aspect	Typical Risks	Controls / Mitigations
Outdated DR plans	Ineffective recovery	Regular testing and updates
Inadequate RTO/RPO definitions	Excessive downtime or data loss	BIA-driven recovery objectives
No alternate site or failover	Extended outage	Hot/warm site strategy, cloud DR
Poor staff readiness	Confusion during crisis	DR drills, tabletop exercises

Resiliency tie-in: The cornerstone of **corrective controls**, ensuring survival after severe disruption.

INTEGRATED UNIFIED RISK MAP

- These domains together form a comprehensive operational risk picture
 - A well-built map will
 - Link each domain to critical business services
 - Classify risks as preventive, detective, or corrective
 - Assign ownership: who monitors, who remediates
 - Integrate with SOPs and maturity models
- Example
 - Preventive: Patching, Change Control, Access
 - Detective: Monitoring, Logging, Incident Response
 - Corrective: Backup/Restore, DR/BCP, Problem Management

RISK MAPPING AND PROCESS MATURITY

- In operational risk and resilience management
 - Risk mapping shows where vulnerabilities and control gaps exist
 - Process maturity indicates how well those risks are being managed through consistent, repeatable, and measurable processes.
 - A risk map tells you what can go wrong
 - Process maturity tells you how ready you are to handle it

RISK MAPPING AND PROCESS MATURITY

Stage	Focus	Risk Mapping Role	Process Maturity Indicator
Identify	What could go wrong?	Map risks across operational domains (patching, access, backup, etc.)	Reactive awareness of risks — ad hoc controls
Assess	How severe are the risks?	Assign likelihood and impact; visualize via heat maps	Risks are categorized but not consistently managed
Control	What mitigations exist?	Map controls (preventive, detective, corrective)	Basic controls in place but not standardized
Optimize	Are controls working effectively?	Link map to metrics (e.g., MTTR, incident count)	Continuous improvement and measurement
Integrate	Is risk management embedded in daily ops?	Integrate risk maps into SOPs, audits, and decision-making	Mature processes with embedded risk culture

RISK MAPPING AND PROCESS MATURITY

Maturity Level	Description	Risk Mapping Behavior	Example Indicators
Level 1 – Initial (Ad Hoc)	Processes are informal, undocumented	Risks identified only after incidents	No consistent patch tracking, reactive recovery
Level 2 – Managed (Repeatable)	Basic procedures exist	Simple risk lists or spreadsheets used	Manual access reviews, basic monitoring alerts
Level 3 – Defined (Documented & Standardized)	SOPs and controls formally defined	Regular risk mapping as part of operations reviews	Defined patch schedules, DR drills
Level 4 – Quantitatively Managed	Metrics used to measure performance	Risk maps linked to KPIs and dashboards	Automated patch compliance, SLA metrics, residual risk tracking
Level 5 – Optimizing (Continuous Improvement)	Continuous feedback and learning culture	Dynamic, real-time risk mapping integrated into governance	AI-driven monitoring, continuous process tuning

RISK MAPPING AND PROCESS MATURITY

Benefit	Description
Consistency	Mature processes ensure risks are assessed and recorded the same way across teams.
Accountability	Defined ownership and roles improve control effectiveness.
Measurability	Maturity enables tracking of residual risk and control performance using metrics.
Feedback loops	Lessons learned from incidents feed back into updated SOPs and risk maps.
Continuous improvement	Mature organizations evolve risk maps as systems, threats, and technologies change.

Q&A AND OPEN DISCUSSION

