RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RESILIENCE

This section is a more detailed look at operational resilience along the dimensions of

- Business
- Technology
- Data
- Cyber

OPERATIONAL RESILIENCE

- DRI definition
  - The ability of an organization to anticipate, prepare for, respond to, and adapt to incremental changes and sudden disruptions in order to survive and prosper
- ISACA/Basel definition
  - The organization's ability to deliver critical operations and services through disruption, safeguarding customers, markets, and the financial system
- Traditional business continuity and disaster recovery
  - Focus on getting systems back online after an incident
  - Restoring operations to their prior state

OPERATIONAL RESILIENCE

- Operational resilience
  - Represents a more mature and proactive approach
  - It assumes that disruptions will happen but the organization's mission, values, and trust relationships must persist regardless of adverse events
  - Resilience protects what the organization does (mission), not just what it uses (systems)
- Continuity of Mission
  - The idea that the purpose of the organization must not stop, even when individual systems or functions fail
  - Operational resilience ensures that critical services, those that define why the organization exists, remain deliverable under duress
    - For example, a bank's mission is to maintain financial confidence and liquidity for its customers
    - Even during a cyberattack or data center failure, deposits, transactions, and access to funds must continue
  - Designing operations so that core functions are preserved, not just infrastructure restored
    - For example: alternate processing, manual workarounds, and prioritized resource allocation

OPERATIONAL RESILIENCE

- Continuity of trust
  - Trust is a critical, often overlooked asset in operational resilience
  - Customers, partners, regulators must believe the organization can withstand stress and remain reliable
  - A company that continues to operate transparently and responsibly during crises enhances its reputational capital and goodwill
  - Repeated outages or inconsistent communication erode confidence and can lead to regulatory scrutiny or customer flight
  - Maintaining trust requires transparent communication, ethical response behaviors, and robust governance during incidents
  - Resilience is about preserving confidence as well as preserving capability

OPERATIONAL RESILIENCE

- Continuity of adaptability
  - Resilience also depends on the adaptability of the organization to rapidly changing work
    - For example: Cyber attacks, AI technology, pandemics, supply-chain disruptions
  - Adaptability is learning from disruptions, adjusting processes to be more reliable
    - Refining preventive and corrective controls, updating SOPs, and evolving architectures is response to disruption
    - Maturity principle of continuous improvement (discussed later)
    - Prepare → Respond → Recover → Adapt → Evolve.
  - High maturity organizations continuously integrate lessons learned into operations, technology, and governance
  - Operational resilience is not static but must continuously evolve

COMPARISON

Traditional Recovery	Operational Resilience
Restores systems and data after failure	Sustains critical missions and services during and after disruption
Focuses on technical repair	Integrates people, process, and trust into continuity
Ends at "back to normal"	Continues through adaptation and improvement
Measures uptime and restoration	Measures service continuity, stakeholder confidence, and organizational learning

DIMENSIONS

Layer	Purpose	Key Question
Business Resilience	Maintain essential business services under disruption	*Can the organization continue serving customers?*
Technology (IT) Resilience	Ensure IT systems and infrastructure remain available and recoverable	*Can technology support business continuity?*
Data Resilience	Protect, preserve, and recover data integrity, availability, and confidentiality	*Can we trust our data during and after an incident?*
Cyber Resilience	Maintain secure operations under cyberattack or compromise	*Can we withstand and recover from cyber threats?*

Each builds upon the other: **cyber resilience protects data**, **data resilience enables IT recovery**, and **IT resilience supports business continuity**.

THE LAYERS

- Business resilience
  - Capacity of an organization to maintain critical business functions and services during disruption through effective planning, communication, and alternate delivery mechanisms
  - Core focus areas
    - Business Impact Analysis (BIA)
    - Continuity planning and testing
    - Workforce resilience (cross-training, leadership)
    - Supplier and third-party continuity
    - Alternate site and process strategies
    - Crisis communication and stakeholder management

THE LAYERS

- Business resilience
  - Best practices
    - Define critical functions and their Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)
    - Develop continuity playbooks for essential processes (payments, trading, claims, logistics)
    - Regularly exercise continuity plans under different disruption scenarios
    - Use lessons learned to continually refine plans
  - Example
    - A bank’s Business Resilience Plan ensures that payment clearing and customer support continue even if the main data center or call center goes offline
    - Through using remote access, alternate staffing, and branch-level contingencies

THE LAYERS

- Technology (IT) resilience
  - The ability of IT systems, infrastructure, and applications to resist, absorb, recover from, and adapt to disruptions while maintaining essential business services.\
  - Core focus areas
    - Redundant and failover infrastructure
    - Backup and recovery mechanisms
    - High-availability and clustering designs
    - Cloud resilience and multi-region deployments
    - Testing of failover procedures and RTO/RPO validation
    - Automation in recovery (Infrastructure as Code, orchestration)

THE LAYERS

- Technology (IT) resilience
  - Best practices
    - Implement disaster recovery (DR) and high-availability architectures based on what is critical to the business
    - Use chaos engineering to validate system response to failure
    - Integrate DevOps pipelines for resilience testing during builds
    - Maintain asset and dependency mapping to identify critical system relationships
  - Example
    - A trading platform replicates transaction data across regions and performs automated switchover to a hot site within 30 seconds to maintain compliance with 99.99% uptime requirements

THE LAYERS

- Data resilience
  - The ability to preserve and restore data integrity, confidentiality, and availability during and after disruptions
    - For example: data corruption, accidental or malicious deletion, ransomware events.
  - Core focus areas
    - Data backup, replication, and retention
    - Immutable storage and air-gapped backups
    - Data classification and prioritization
    - Encryption and data loss prevention (DLP)
    - Data governance and lineage tracking
    - Data validation and integrity testing

THE LAYERS

- Data resilience
  - Best practices
    - Maintain 3-2-1 backup strategy (3 copies, 2 media, 1 off-site)
    - Test restore processes regularly; backups are only as good as verified recoveries
    - Classify data based on criticality; for example, Tier 1 for regulatory and customer data)
    - Use immutable snapshots and continuous replication for critical data sets
    - Integrate data recovery drills into continuity and cyber incident tests
  - Example
    - A hospital's EHR (Electronic Health Records) system uses daily encrypted backups and maintains redundant copies in two cloud regions
    - Periodic test restores validate recovery times within RTOs

THE LAYERS

- Cyber resilience
  - Cyber resilience combines information security and continuity disciplines to ensure the organization can withstand, detect, respond to, and recover from cyber incidents without severe impact
  - Core focus areas
    - Threat detection and response (SIEM, SOC, EDR)
    - Identity and access management (MFA, least privilege)
    - Network segmentation and zero trust architecture
    - Security patching and vulnerability management
    - Incident response and recovery planning
    - Integration with business continuity and crisis management

THE LAYERS

- Cyber resilience
  - Best practices
    - Implement Defense-in-Depth architecture and Zero Trust principles
    - Establish Incident Response SOPs with defined roles and escalation paths
    - Use cyber incident simulations (tabletop exercises) involving IT, legal, and executive teams
    - Ensure backup systems are logically separated to prevent ransomware encryption spread
    - Apply DRI's lifecycle approach: prepare → detect → respond → recover → adapt
  - Example
    - A major retailer withstands a ransomware attack because its cyber resilience plan isolates infected systems, activates clean backups, and restores operations within 6 hours, all coordinated via its incident response SOP

DEFINITIONS

- SIEM: Security Information and Event Management
  - SIEM is a technology platform that collects, correlates, and analyzes security-related data from across an organization's IT environment to investigate, and respond to security incidents
    - Includes servers, firewalls, network devices, and applications
  - Purpose
    - To provide centralized visibility into security events and potential threats
    - To correlate patterns across multiple systems that may indicate attacks or policy violations
    - To support real-time alerting, incident response, and compliance reporting
  - Key capabilities
    - Log aggregation: Collects logs from across the enterprise
    - Event correlation: Connects multiple indicators to detect complex threats
    - Alerting and dashboards: Real-time monitoring for suspicious activity
    - Forensics and reporting: Provides evidence for audits and investigations

DEFINITIONS

- EDR: Endpoint Detection and Response
  - Cybersecurity technology that monitors and analyzes endpoint activities to detect, investigate, and respond to suspicious behavior or malware in real time
    - For example: laptops, servers, mobile devices, IoT)
  - Purpose
    - To provide detailed visibility into endpoint behavior and attack chains
    - To support rapid containment and remediation actions
    - For example: isolate device, kill process
  - Key capabilities
    - Real-time monitoring: Continuous tracking of process execution, registry changes, network connections, etc.
    - Behavioral analytics: Detect anomalies or suspicious activity patterns
    - Automated response: Quarantine devices or block malicious actions instantly
    - Forensics: Provide timeline and evidence for post-incident analysis

DEFINITIONS

- Chaos engineering
  - Deliberately injecting controlled failures or disruptions into systems to test their resilience, reliability, and ability to recover under real-world conditions
    - Based on the idea that the best way to build fully resilient systems is to experiment with failure before it happens in production, identify weaknesses, and fix them proactively
  - Rationale
    - Modern IT systems are complex.
    - For example: especially those running in the cloud, with microservices, containers, and distributed architectures
    - Even small component failures can cascade into large-scale outages if the system isn't designed for fault tolerance
  - Chaos engineering goals
    - Reveals hidden dependencies and failure modes
    - Validates assumptions about redundancy, failover, and recovery mechanisms
    - Improves operational resilience by testing how people, processes, and technology respond to stress
    - Shift from preventing failure to preparing for it by experiencing it

DEFINITIONS

- Chaos engineering
  - Chaos engineering is structured and scientific, not creating random damage
  - Start from a steady state
    - Define normal system behavior (e.g., latency, throughput, error rate)
  - Form a hypothesis
    - Example: “If one database node fails, the application will continue serving users via the replica”
  - Introduce controlled disruption
    - Simulate real-world faults such as network latency, instance crashes, or service outages
  - Observe and measure
    - Monitor system metrics and user experience for deviation from the steady state
  - Learn and improve
    - Identify weaknesses, fix them, and re-test until the system performs predictably under stress

CHAOS EXAMPLES

Failure Type	Example Experiment	Resilience Focus
Infrastructure Failure	Shut down random virtual machines or containers	Validates redundancy and failover
Network Latency / Partition	Introduce artificial delay or cut off connections between services	Tests service timeout and retry logic
Dependency Outage	Disable external API or database temporarily	Verifies graceful degradation and fallback mechanisms
High Load / Resource Exhaustion	Simulate CPU or memory spikes	Tests auto-scaling and performance under stress
Configuration Error	Deploy invalid configuration	Tests validation and rollback procedures
Security Incident Simulation	Inject mock credentials or simulate a ransomware lock	Tests response, alerting, and recovery processes

CHAOS TOOLS

Tool	Description
Netflix Chaos Monkey	Randomly terminates production instances to ensure fault tolerance.
Gremlin	Commercial platform for running controlled chaos experiments (network, CPU, disk, etc.).
AWS Fault Injection Simulator (FIS)	Cloud-native tool for injecting faults into AWS environments safely.
Azure Chaos Studio	Microsoft's managed chaos engineering service for Azure workloads.
LitmusChaos / Chaos Mesh	Open-source chaos frameworks for Kubernetes environments.

CHAOS RESILIENCE SUPPORT

Resilience Dimension	Chaos Engineering Contribution
Technology Resilience	Tests infrastructure redundancy, failover, and recovery under stress.
Data Resilience	Validates backup and replication mechanisms.
Cyber Resilience	Assesses security monitoring and response under simulated attacks.
Business Resilience	Confirms that critical services remain operational even when underlying systems fail.
Organizational Resilience	Improves staff readiness, incident response, and cross-team coordination.

INTEGRATION AND INTERDEPENDENCE

Resilience Layer	Depends On	Supports
Business Resilience	Tech & Data availability	Customer service continuity
Tech Resilience	Data integrity, Cyber defense	Business continuity
Data Resilience	Cyber resilience, Governance	IT and regulatory compliance
Cyber Resilience	Processes, Technology, People	All other resilience layers

FRAMEWORK ALIGNMENT

Framework / Standard	Relevant Elements
DRI Professional Practices (PP4–PP8)	Risk Evaluation, Business Impact Analysis, Incident Response, Implementation, Testing & Maintenance
ISACA COBIT / IT Risk Framework	Aligns IT processes and controls with business continuity objectives
ISO 22316	Principles of Organizational Resilience (leadership, shared purpose, continual improvement)
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems
NIST Cybersecurity Framework (CSF)	Identify → Protect → Detect → Respond → Recover
Basel Committee / BCBS 239	Principles for operational resilience and critical service delivery
CERT-RMM	Process maturity model linking IT, security, and operational resilience capabilities

Q&A AND OPEN DISCUSSION