RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RECOVERY MODELS

This section is an introduction to

- Recovery models and processes
- Business recovery lifecycles

OPERATIONAL RESILIENCE

- After disruptions from any cause
  - An organization must be able to recover essential functions quickly and effectively
  - Recovery models
    - Define how systems, processes, and business functions are restored after an incident: how resilience is implemented
  - The business recovery life cycle
    - A structured process for achieving resilience
    - From identifying critical activities to testing recovery capabilities
- These form the core of operational resilience
  - Ensures that a bank or financial institution can continue serving customers, protect assets, and meet regulatory obligations under stress

RECOVERY MODELS

- Recovery model
  - A defined approach or architecture for restoring IT systems, data, and business operations to a functional state following a disruption
  - Determine where, how, and to what level recovery occurs
- Resilience metrics
  - Models are guided by the resilience measure we saw earlier
  - RTO (Recovery Time Objective)
    - The maximum acceptable time a process or system can be unavailable before serious impact occurs
  - RPO (Recovery Point Objective)
    - The maximum acceptable amount of data loss measured in time (e.g., 15 minutes, 4 hours)

RECOVERY MODELS

- Resilience metrics
  - Models are guided by the resilience measure we saw earlier
  - MAO (Maximum Acceptable Outage)
    - The total time a process can be disrupted before organizational viability is threatened
  - MBCO (Minimum Business Continuity Objective)
    - The minimum level of output or service that must be maintained during disruption
  - Recovery Tier / Strategy
    - A structured level defining recovery speed and infrastructure complexity (e.g., hot site, warm site, cold site)

RECOVERY MODEL TYPES

Recovery Model	Description	Typical RTO / RPO	Example
Hot Site	Fully operational site with mirrored systems, real-time data replication, and staff readiness.	RTO: Minutes to <1 hour RPO: Near zero	Tier 1 banking data center using synchronous replication between regions.
Warm Site	Partially equipped site with hardware and connectivity ready but requires data restoration and configuration.	RTO: 4–8 hours RPO: Few hours	Backup servers at DR site loaded from last backup.
Cold Site	Facility with power and network but no active equipment or data; requires full setup.	RTO: 24–72 hours RPO: 24+ hours	Leased floor space for emergency setup after a disaster.
Cloud Recovery	Uses cloud platforms to dynamically provision systems from backup or infrastructure as code (IaaC).	RTO: Varies (minutes to hours) RPO: Configurable	AWS Elastic Disaster Recovery or Azure Site Recovery for hybrid workloads.
Reciprocal Agreement	Mutual arrangement with another organization to share facilities during crisis.	RTO/RPO depend on setup	Two banks sharing backup call centers.
Mobile Recovery Site	Mobile data center or office brought on-site with connectivity and hardware.	RTO: 24–48 hours	Mobile trailers deployed during hurricane recovery.

RECOVERY PROCESS FLOW

- Recovery Process Flow
  - The operational execution of resilience
  - The step-by-step progression
    - From detecting a disruption through restoring normal business operations
    - Then updating the appropriate controls
  - The flow
    - *Detection:* Recognize the disruption or incident
    - *Notification*: Escalate to recovery or crisis teams
    - *Assessment*: Analyze impact and decide if recovery plan activation is required
    - *Activation*: Initiate recovery processes (failover, backup restore, alternate site)
    - *Restoration*: Restore systems and business operations
    - *Verification*: Validate restored systems for accuracy and completeness
    - *Return to Normal*: Transition from recovery to standard operations
    - *Post-Incident Review:* Evaluate performance and improve plans

RECOVERY PROCESS FLOW

- Detection
  - Identify that a disruptive event, system fault, or threat condition has occurred and determine its potential to affect business operations
  - Key activities
    - Continuous monitoring of systems, applications, facilities, and environmental conditions
    - Use of SIEM, AIOps, or observability tools to detect anomalies, security events, or hardware failures
    - Event correlation and severity classification (e.g., minor incident vs. critical outage)
    - Notification from internal staff, vendors, or customers (incident reporting channels)
  - Responsible roles
    - Network Operations Center (NOC)
    - Security Operations Center (SOC)
    - Monitoring / Site Reliability Engineers (SREs)
  - Resilience
    - Early detection reduces Mean Time to Detect (MTTD), minimizing downtime and data loss
    - Timely detection is a preventive and detective control

RECOVERY PROCESS FLOW

- Notification
  - Alert the appropriate response and recovery teams so that decision-making and containment actions begin immediately.
  - Key activities
    - Trigger automated or manual incident escalation workflows via service management tools
    - Notify Incident Response Team, Crisis Management Team, Communications, and Executive Leadership.
    - Maintain communication channels: email, phone trees, emergency alert systems, or crisis collaboration platforms
    - Document timestamps for all notifications to ensure traceability.
  - Responsible roles
    - Incident Commander or Recovery Coordinator
    - IT Operations Manager
    - Business Continuity Manager (BCM)
  - Resilience
    - Proper notification prevents decision delays and chaos
    - Clear escalation protocols are part of DRII's "Incident Response" practice, ensuring consistent activation

RECOVERY PROCESS FLOW

- Assessment
  - Evaluate scope, severity, and potential impact to decide if recovery plans should be activated
  - Key activities
    - Conduct a rapid impact analysis: Which systems, business processes, and customers are affected?
    - Compare disruption with RTO and RPO thresholds
    - Check for regulatory implications, for example, if a disruption affects financial reporting or data privacy
    - Determine whether to escalate from incident management to crisis management or disaster recovery activation
    - Engage the Business Impact Analysis (BIA) data to prioritize recovery sequence
  - Responsible roles
    - Crisis Manager / Incident Commander
    - IT Disaster Recovery Lead
    - Business Function Leaders (process owners)
  - Resilience
    - This stage ensures proportionate response
    - Avoiding overreaction to minor issues while guaranteeing timely activation for critical disruptions

RECOVERY PROCESS FLOW

- Activation
  - Formally declare a recovery event and launch the relevant recovery strategies, procedures, and teams
  - Key activities
    - Activate Disaster Recovery (DR) and Business Continuity (BC) plans
    - Mobilize alternate facilities, hot sites, or cloud recovery environments
    - Begin system failover, backup restoration, or workload redirection (e.g., to secondary data center or cloud region)
    - Initiate manual workarounds for critical business processes if IT systems are unavailable
    - Establish command centers or war rooms to coordinate communication and actions
  - Responsible roles
    - Business Continuity Manager
    - IT DR Team and Infrastructure Leads
    - Crisis Communications Officer
  - Resilience
    - Execution of well-defined, documented, and rehearsed plans that allow faster and safer recovery

RECOVERY PROCESS FLOW

- Restoration
  - Return affected systems and processes to a functional state that allows essential operations to resume
  - Key activities
    - Execute technical recovery procedures: restoring servers, databases, network links, and applications in prioritized sequence
    - Validate data integrity from backups or replicas
    - Coordinate user acceptance testing (UAT) or “sanity checks” to confirm functionality
    - Reconnect dependent systems and third-party integration
    - Resume key business functions under controlled conditions like limited customer traffic
  - Responsible roles
    - IT DR Engineers and Database Administrators
    - Application Owners
    - Business Recovery Coordinators
  - Resilience
    - Restoration is the core of operational resilience
    - Metrics like RTO compliance and service restoration SLA are key resilience indicators

RECOVERY PROCESS FLOW

- Verification
  - Ensure that restored systems, data, and processes are fully functional, accurate, and safe before resuming normal operations
  - Key activities
    - Verify transactional accuracy and reconcile financial data
    - Run integrity checks (hash comparisons, audit logs)
    - Perform security revalidation: re-enable access controls, patch systems if necessary
    - Conduct post-recovery testing (connectivity, workflows, reports)
    - Obtain business owner sign-off confirming system readiness
  - Responsible roles
    - QA / Testing Teams
    - Information Security Officers
    - Business Process Owners
  - Resilience:
    - Verification prevents secondary failures caused by incomplete restoration

RECOVERY PROCESS FLOW

- Return to normal
  - Move from temporary recovery configurations back to normal, stable production operations, closing out crisis mode
  - Key activities
    - Decommission temporary systems, failover environments, or alternate site.
    - Validate synchronization between recovered and primary systems
    - Resume standard SLAs and monitoring thresholds
    - Communicate “all clear” internally and externally to customers, partners, and regulators
    - Reassign staff to standard duties; document resource usage
  - Responsible roles
    - Operations Managers
    - Recovery Coordinators
    - Communications & HR (for workforce normalization)
  - Resilience
    - Smooth transition avoids “recovery drift”, where organizations operate indefinitely in degraded or improvised states

RECOVERY PROCESS FLOW

- Post-incident review
  - Capture lessons learned, assess response performance, and strengthen resilience for the future
  - Key activities
    - Conduct After-Action Reviews (AARs) within days of the event
    - Document root causes, control gaps, and timeline of events
    - Compare actual RTO/RPO vs. targets; identify deviations
    - Recommend process improvements, automation, or additional controls
    - Update recovery plans, training materials, and BIA data
    - Report results to governance and compliance committees
  - Responsible roles
    - Business Continuity Office (BCO)
    - Risk & Compliance Teams
    - IT and Business Stakeholders
  - Resilience
    - Closes the loop in the resilience lifecycle: transforming incidents into learning opportunities

RECOVERY PROCESS SUMMARY

Stage	Purpose	Key Metric	Resilience Focus
1. Detection	Identify disruption quickly.	MTTD (Mean Time to Detect)	Early warning and situational awareness.
2. Notification	Escalate promptly to right teams.	MTTA (Mean Time to Acknowledge)	Speed of coordination.
3. Assessment	Evaluate impact and need for activation.	Decision Time to Activation	Data-driven escalation.
4. Activation	Launch recovery strategies and plans.	Activation Time	Controlled, rapid execution.
5. Restoration	Restore systems and data.	RTO, RPO compliance	Technical recovery and continuity.
6. Verification	Validate accuracy and integrity.	% Successful Verification	Trust and reliability.
7. Return to Normal	Transition back to steady-state.	Time to Stabilization	Normalized operations and monitoring.
8. Post-Incident Review	Capture lessons, improve plans.	Closure Time for Corrective Actions	Continuous improvement and adaptive resilience.

LAYERS OF RECOVERY

Layer	Recovery Focus	Example
Data Recovery	Restoring data to last good state (RPO focus)	Database restore from backups or replicas
System Recovery	Restoring applications, servers, or virtual environments	Rebuilding a failed virtual machine
Network Recovery	Reconnecting users, sites, and external partners	Restoring VPN or WAN links
Business Process Recovery	Resuming core functions and workflows	Restarting payment processing after outage
Facility Recovery	Relocating operations to alternate site	Moving staff to backup office or cloud-hosted workspace
People / Workforce Recovery	Enabling staff to work safely from alternate locations	Work-from-home or co-location plans

BUSINESS RECOVERY LIFE CYCLE

- Business Recovery life cycle consists of eight interdependent practices grouped into three phases

Phase	Practice	Purpose
Program Initiation and Management	1. Program Initiation & Management	Establish governance, policies, and sponsorship for recovery planning.
Risk & Impact Assessment	2. Risk Assessment 3. Business Impact Analysis (BIA)	Identify potential threats and determine which functions are critical.
Strategy & Plan Development	4. Business Continuity Strategies 5. Incident Response 6. Plan Implementation	Define recovery models, incident response steps, and detailed plans.
Validation & Maintenance	7. Awareness & Training 8. Testing, Evaluation & Maintenance	Ensure staff readiness and continuous improvement.

BUSINESS RECOVERY LIFE CYCLE

- Business recovery life cycle
  - Program initiation and governance
    - Secure executive sponsorship and define scope
    - Assign roles: Business Continuity Manager, Recovery Coordinator, IT DR Lead
    - Align with enterprise risk management and regulatory requirements (e.g., FFIEC, OCC)
  - Risk assessment
    - Identify threats (cyberattacks, power failure, flood, supplier outage)
    - Evaluate likelihood and impact
    - Identify single points of failure in critical operations
  - Business impact analysis (BIA)
    - Determine critical functions and their dependencies (systems, people, vendors)
    - Establish RTOs and RPOs
    - Prioritize recovery order (what must come back first)

BUSINESS RECOVERY LIFE CYCLE

- Business recovery life cycle
  - Strategy development
    - Select appropriate recovery models (hot, warm, cloud, etc.) based on BIA results
    - Balance cost vs. recovery speed
    - Document technology, data, and process recovery strategies
  - Plan development and implementation
    - Create detailed Recovery Procedures / SOPs:
      - Activation criteria
      - Communication protocols
      - Technical recovery steps
      - Validation checkpoints
    - Coordinate with IT, facilities, HR, and external vendors.

BUSINESS RECOVERY LIFE CYCLE

- Business recovery life cycle
  - Awareness, training, and communication
    - Conduct regular training for recovery and crisis response teams
    - Educate employees on roles during incidents
    - Maintain internal and external contact lists
  - Testing and exercising, Validate recovery plans through
    - Tabletop exercises (discussion-based)
    - Functional drills (partial system tests)
    - Full-scale simulations (end-to-end recovery)
  - Measure performance against RTO/RPO and identify improvements

BUSINESS RECOVERY LIFE CYCLE

- Business recovery life cycle
  - Maintenance and continuous improvement
    - Review and update recovery plans regularly (at least annually)
    - Incorporate lessons learned from incidents and tests
    - Adjust to organizational changes, new systems, or threats

RISK AND RESILIENCE

Aspect	Recovery Lifecycle Contribution	Resilience Impact
Risk Identification	Through Risk Assessment & BIA	Informs control design and investment prioritization
Operational Preparedness	Defined recovery models and tested procedures	Reduces downtime and data loss
Response Capability	Clear activation and communication steps	Faster containment, less confusion
Recovery Capability	Verified failover and restoration plans	Predictable service restoration
Adaptation / Learning	Post-incident review and plan updates	Continuous resilience improvement

COMMON ERRORS

Challenge	Explanation	Mitigation
Confusing backup with recovery	Backups store data; recovery restores service continuity.	Integrate both into tested recovery scenarios.
Lack of testing	Plans look good on paper but fail in practice.	Schedule realistic, scenario-based tests.
Overly technical focus	Ignoring business process dependencies.	Include both IT and business functions in planning.
No executive support	Plans remain underfunded or unprioritized.	Tie recovery outcomes to regulatory and reputational risk.
Static plans	Plans not updated as systems evolve.	Embed maintenance as part of governance cycle.

SUMMARY

Element	Definition	Resilience Value
Recovery Model	Framework defining how systems and business functions are restored.	Determines speed, completeness, and reliability of recovery.
Recovery Process	The sequence of actions triggered after disruption.	Provides structure and accountability.
Business Recovery Lifecycle	The continuous program to plan, test, and improve recovery.	Embeds resilience into organizational DNA.

Q&A AND OPEN DISCUSSION