Final Exam: Risk Mitigation Strategies

CJ McDonald

Department of Cybersecurity, Old Dominion University

CYSE 430: Intro to Cyber Risk Management

Professor Hamza Demirel

May 4, 2025

Organizations today face a relentless array of threats capable of interrupting critical functions without warning. From severe weather events that can sever supply chains and damage facilities to sophisticated cyberattacks that can freeze networks and expose sensitive data, the potential for disruptive incidents is ever‑present. To guard against such interruptions, an organization must first invest in a comprehensive assessment of its operations to understand which activities cannot withstand even brief delays. This effort typically brings together representatives from every unit—IT specialists, process owners, human resources leaders, finance managers, procurement officers, and executive sponsors—to ensure that no blind spots remain in the analysis. Guided interviews and structured questionnaires reveal how long each process can function without its supporting systems and what substitutes might exist if primary resources go offline.

During these collaborative sessions, participants map each business process to its underlying dependencies: physical infrastructure, software applications, data repositories, human skills, third‑party services, and regulatory constraints. They quantify potential losses across dimensions such as lost revenue per hour of downtime, contractual penalties for missed service‑level agreements, and intangible reputational damage that could erode customer loyalty. By defining recovery time objectives—the maximum downtime tolerable before losses become unacceptable—and recovery point objectives—the maximum amount of data loss a function can tolerate—stakeholders establish clear thresholds that will guide all subsequent planning. Whether a process can function with manual workarounds for a few hours, requires rapid system failover, or demands near‑zero downtime, these recovery objectives dictate the level of investment in resiliency measures, from redundant hardware to geographically dispersed data centers.

Once the assessment yields a prioritized list of critical functions and recovery objectives, the organization shifts toward crafting practical continuity measures designed to maintain operations during unexpected events. This phase blends creative problem solving with rigorous documentation. Teams devise remote-work policies that allow employees to continue processing transactions from alternate locations if physical offices are compromised. Cross-training programs ensure that no single individual holds the exclusive knowledge needed to run a vital process. Agreements with secondary suppliers provide alternative sources for essential materials or services when primary vendors are affected by disruptions. In each case, detailed procedures specify exactly how the organization will pivot to these secondary modes—who authorizes the switch, how employees receive instructions, and how leadership monitors progress.

To keep continuity plans evergreen, organizations schedule a variety of exercises that stress-test assumptions and reveal unforeseen gaps. Walkthroughs—where participants review procedures step by step—help eliminate ambiguities in the documentation. Tabletop simulations—where teams role-play decision-making in a war room setting—expose communication bottlenecks and misaligned priorities. Technical failover drills, whether on a subset of infrastructure or across entire systems, validate that automated switching mechanisms work as intended and highlight areas needing improved orchestration or capacity. After each exercise, leadership conducts a frank discussion of what succeeded and where breakdowns occurred, then updates the playbooks accordingly. By weaving lessons learned back into the planning cycle, the organization fosters a culture of continuous improvement rather than allowing contingency plans to grow stale.

Underlying any credible continuity capability is a robust strategy for restoring technology systems, since virtually every major business function relies on digital services. To build this

capability, organizations maintain an exhaustive inventory of servers, network devices, application platforms, and data stores, along with their configurations and interdependencies. Armed with this inventory, technical teams design backup and replication schemes calibrated to the recovery objectives set during the impact analysis. For applications with less stringent data‑loss tolerances, nightly full backups stored off‑site may suffice. For systems requiring near‑real‑time replication, technologies such as continuous data replication or storage snapshots paired with automated failover orchestration ensure that a standby environment can take over with minimal manual intervention.

Every recovery strategy is codified in runbooks—precise, command‑level guides that detail each step of system restoration. A runbook for a critical database might enumerate console commands to initialize a new server instance, apply security patches, mount storage volumes from encrypted backup snapshots, and import the transaction logs needed to bring the database up to the most recent permissible point. At key junctures, validation checks confirm service responsiveness and data integrity before allowing end users to resume normal operations. The runbooks themselves are version‑controlled and stored in secure, accessible repositories so that they remain synchronized with evolving system architectures and software updates.

While continuity and disaster recovery planning address the mechanical side of keeping lights on, the unpredictable realm of cybersecurity incidents demands equally rigorous preparation. Organizations form specialized response teams tasked with handling incidents from the moment an anomaly is detected until systems are fully restored and fortified against similar attacks. The team’s charter lays out clear roles: an incident leader to orchestrate the response, forensic analysts to preserve evidence, IT operations experts to apply containment measures,

legal advisors to ensure regulatory compliance, and communications specialists to manage both internal stakeholders and external audiences.

Detection hinges on a combination of automated monitoring platforms and human expertise. Security information and event management systems aggregate logs from firewalls, intrusion detection sensors, servers, and applications, applying analytics to surface patterns indicative of malicious activity. Endpoint detection tools watch for suspicious behaviors—unusual file encryption, privilege escalation attempts, or anomalous network connections—triggering alerts for human review. When a credible threat emerges, the response team springs into action by isolating affected systems—cutting them off from the network or routing traffic through quarantine segments—while forensic imaging captures disk snapshots for later analysis.

Containment and eradication carry ethical and operational weight. Technical teams apply patches or configuration changes to close exploited vulnerabilities, remove malware binaries, and reset compromised credentials. At the same time, legal and compliance functions evaluate notification obligations under data-breach regulations, coordinating external disclosures to customers, regulators, and law enforcement as needed. Transparency and timeliness underpin trust—both within the organization and with external partners—so pre-approved communication templates accelerate the drafting of notifications while ensuring consistency with legal requirements.

Recovery from a security incident often leverages the backups and runbooks developed for disaster recovery. With clean copies of affected systems, technical teams rebuild production environments under the supervision of forensic experts who verify that no malicious artifacts persist. Enhanced monitoring and threat hunting activities continue in the immediate aftermath to

confirm that attacks have been fully eradicated. Following restoration, the team conducts a comprehensive root-cause analysis to document how the breach occurred and which control gaps contributed, then integrates these findings into the broader continuity and security strategies to reduce the likelihood of future recurrence.

The true value of these four elements—impact assessment, continuity planning, disaster recovery, and incident response—emerges when they converge under unified governance. A resilience committee comprised of senior leaders from across the organization oversees ongoing risk management, setting policy, funding initiatives, and resolving conflicts between business units. This committee maintains a central repository where the latest process maps, recovery objectives, runbooks, and response playbooks reside. Any organizational change—launching a new product line, migrating to a different cloud provider, or restructuring internal teams—automatically triggers a review cycle across all resilience artifacts, ensuring that each plan reflects the current business context and technology environment.

Periodic audits against established standards—be they international frameworks like ISO 22301 for continuity management or industry best practices such as NIST SP 800-34 for disaster recovery planning—provide external validation and catalyze improvements. Metrics such as average downtime per incident, percentage of recovery objectives met within targets, and mean time to detect and contain security breaches offer tangible measures of program maturity. By reporting these metrics to executive leadership and the board, the resilience team maintains visibility into risk posture and secures ongoing investment in critical capabilities.

In an era when the pace of change and complexity of threats escalate continuously, resilience is not a one-time project but an enduring discipline. Organizations that treat this work

as a living program—characterized by repeated cycles of assessment, planning, testing, and refinement—stand the best chance of withstanding the next major disruption. They cultivate a culture in which employees at every level value readiness and collaboration, where contingency plans are trusted resources rather than forgotten binders, and where failures spark active learning rather than finger-pointing. Through this holistic and adaptive approach, companies can transform uncertainty into strength, preserving operational continuity, safeguarding data integrity, and maintaining stakeholder confidence, no matter what challenges arise.

Works Cited

Panko, R. R. (2021). Business impact analysis and risk assessment. In *Corporate computer security* (4th ed., pp. 435–462). Pearson.