Conduct a Risk Assessment, Develop a Business Impact Analysis and Business Continuity Plan

Ryan Coon

CYB-650

Dr. Howard Goodman

August 6, 2025

**Critical Systems and their Impact on the Organization**

Our organization's core functionality hinges on several critical systems safeguarding sensitive data: financial records, personal information, and confidential health data. The failure of any one of these systems would have catastrophic consequences. Imagine the devastating financial repercussions of a financial system breach—a torrent of lost funds and shattered investor confidence. A compromised personal data system would trigger a crisis of public trust, eroding our reputation and potentially leading to legal action, and a breach of our health data system. The ramifications would be dire, exposing us to significant legal liabilities and reputational damage, potentially resulting in crippling penalties for negligence. The stability and security of these systems are paramount to our organization's survival and success.

**High Risk Findings and Suggested Mitigation Strategies**

A comprehensive qualitative risk assessment significantly enhances an organization's ability to proactively identify and mitigate potential security threats and vulnerabilities within its systems. Our recent vulnerability assessment revealed several critical findings, the most significant being the vulnerability of our financial system to unauthorized access. This vulnerability poses a substantial risk, as a successful breach could expose sensitive customer data, including credit card numbers and bank account details, potentially leading to identity theft and significant financial losses. To mitigate this risk, the organization should immediately implement robust security measures, including but not limited to: advanced intrusion detection systems, multi-factor authentication protocols, and rigorous access control policies. These measures are crucial in fortifying our defenses against potential cyber threats and ensuring the protection of our customers' sensitive financial information. A swift and decisive response is essential to minimize the potential for a catastrophic data breach.

**Identified Cases**

To mitigate limitations on implementable restrictions, comprehensive security protocols must be established across all systems. This involves the robust development and implementation of secure systems for financial, personal data, and healthcare information, each demanding rigorous authentication and verification procedures for all access attempts. Imagine impenetrable fortresses guarding sensitive data—each entry point secured by advanced authentication systems, ensuring only authorized personnel can breach the digital walls. This multi-layered approach will create an unyielding defense against unauthorized intrusions, protecting the integrity of our valuable information assets. The implementation of these measures is not merely a technical undertaking; it is a commitment to safeguarding sensitive information and maintaining the highest standards of security. This proactive approach will transform our digital landscape into a secure and reliable environment, where data privacy and system integrity are paramount.

**Contingency Plan**

Developing a robust contingency plan begins with a meticulous identification of all compliance gaps that could potentially impact the organization. Upon discovery of these vulnerabilities, the hospital must proactively develop and implement comprehensive policies and procedures designed to effectively address each identified gap. The contingency plan must explicitly detail how the organization will maintain unwavering adherence to all relevant laws and regulations, even amidst the chaos of a catastrophic event. Imagine a ship navigating a storm—our contingency plan is the detailed chart, ensuring a safe passage through the turbulent waters of unforeseen circumstances. It's not merely a document; it's a roadmap to operational resilience, guaranteeing the organization's continued compliance and stability, regardless of the challenges faced. This proactive approach ensures that we are not only prepared but also legally and ethically sound in the face of adversity. The implementation of this plan is not merely a reactive measure; it is a testament to our commitment to maintaining the highest standards of compliance and operational integrity, even under duress.

**Cost/Benefit Analysis**

The cost of developing and implementing a comprehensive contingency plan varies based on organizational size and complexity. However, it's crucial to view this expenditure as an investment in organizational resilience. A cost-benefit analysis can help determine the optimal balance between investment and risk mitigation, ensuring that the plan aligns with the organization's specific needs and resources. The potential financial and reputational penalties of not having a plan far outweigh the costs of implementing one.

Key Components of a Solid Plan:

Backups - Regular data backups are non-negotiable.

Supplier Agreements - Make sure our key suppliers have backup plans, too. You don't want to be stuck without essential supplies if something goes wrong.

Alternate Work Locations - Having a backup location is crucial, like having a second home in case your primary one is destroyed.

**Controls that cannot be Implemented**

In the face of a catastrophic event, such as a raging inferno engulfing our building, the immediate disconnection of all equipment becomes an insurmountable task. However, proactive measures, implemented *before* disaster strikes, can significantly mitigate its impact. This comprehensive approach necessitates the meticulous development of three crucial plans: a robust Business Continuity Plan, a meticulously detailed Disaster Recovery Plan, and a swift Incident Response Plan. These interwoven strategies will act as a lifeline, ensuring the organization's continued operation, facilitating a seamless recovery, and providing a rapid response mechanism. The Business Continuity Plan will serve as the cornerstone, meticulously outlining a list of critical functions and assigning responsibility to key personnel. It's also important to note that, according to Bisson (2021), our hospital may not currently have the capacity to encrypt all electronic data. This is a key area for future improvement.

**Compensating Controls**

Compensating controls play a crucial role in allowing noncompliant systems to operate within a secured and compliant environment by providing alternative measures that mitigate risks when primary controls cannot be fully implemented. For instance, if a legacy system cannot meet specific security requirements due to technological limitations, compensating controls can be established to reduce the associated risks to an acceptable level. These controls might include enhanced monitoring, additional access restrictions, or the implementation of robust encryption methods to protect sensitive data. By doing so, organizations can maintain operational continuity while ensuring that the overall security posture remains intact. This approach not only helps in managing compliance gaps but also fosters a culture of proactive risk management, allowing organizations to adapt to evolving threats without compromising their commitment to security and regulatory standards. Ultimately, compensating controls serve as a bridge, enabling noncompliant systems to function effectively within a framework designed to protect sensitive information and uphold compliance obligations.

**Cybersecurity Breach**

To ensure business continuity during cybersecurity breaches, organizations must implement a comprehensive plan encompassing incident response and disaster recovery strategies. The incident response strategy should focus on damage limitation and mitigation, while the disaster recovery strategy prioritizes system and data restoration. Proactive measures, including preventative policies and breach detection protocols, are crucial. While HIPAA compliance significantly reduces the likelihood of a cybersecurity breach at Augusta Medical Hospital, it does not eliminate the risk. Emerging threats, such as zero-day exploits, sophisticated ransomware, and increasingly effective phishing campaigns, can still penetrate even the most robust security systems. The impact of a breach, even within a compliant environment, can be catastrophic, encompassing substantial financial losses from incident response, legal fees, and potential lawsuits; significant reputational damage leading to decreased patient trust and revenue; operational disruption affecting patient care; and severe legal and regulatory penalties for non-compliance, even during breach response. The consequences are amplified by the sensitive nature of patient data and the potential for patient harm, including identity theft and medical fraud. Unlike a non-compliant environment where the likelihood of a breach is significantly higher, a compliant environment, while mitigating risk, necessitates a proactive and multi-layered approach to cybersecurity, encompassing regular security assessments, employee training, and robust incident response planning to address evolving threats and vulnerabilities effectively.

**NIST Framework Controls**

**System Configuration Requirements:**

Firewall Configuration - Configure your firewall to permit only specific incoming and outgoing network traffic by defining allowed IP addresses and ports. This restricts access to your system and prevents unauthorized connections.

Intrusion Detection/Prevention - Install and configure intrusion detection and prevention (IDP) software. IDP systems monitor network traffic for malicious activity, blocking known attacks and alerting you to suspicious behavior.

Anti-Malware Protection - Install and regularly update robust anti-malware software to detect and remove viruses and other malware threats. Ensure regular scans are performed.

Patch Management - Promptly install all critical security patches and updates for your operating system and applications. This is crucial for addressing known vulnerabilities.

Strong Password Policy - Enforce a strong password policy requiring complex, regularly updated passwords for all users. This significantly reduces the risk of unauthorized access.

**System Test Case:**

To rigorously evaluate the system's security posture, the following test cases are proposed:

Unauthorized IP Address Blocking - This test case validates the firewall's configuration to reject connections originating from unauthorized IP addresses. Successful execution demonstrates that only traffic from explicitly permitted IP addresses is accepted, effectively preventing unauthorized access attempts.

Invalid Password Rejection - This test case verifies the system's password policy enforcement. It attempts logins using incorrect passwords. Successful execution confirms that only valid passwords grant access, thereby safeguarding the system from brute-force or credential-based attacks.

Authorized File Download - This test case assesses the system's ability to facilitate legitimate file downloads. A successful execution verifies that authorized users can download files without restriction, demonstrating proper file access controls.

Unauthorized File Execution Prevention - This test case aims to determine whether the system prevents the execution of unauthorized system files. Successful execution confirms the system's ability to thwart malicious code execution attempts.

Software Installation Restriction - This test case evaluates the system's ability to block unauthorized software installations. Successful execution confirms the system's ability to prevent the installation of potentially harmful or unauthorized software.

Malware Detection and Prevention - This test case assesses the effectiveness of the system's anti-malware software. It attempts to introduce a known malware file. Successful execution demonstrates the anti-malware software's ability to detect and prevent malicious code from compromising the system.

References:

Bisson, David. “Compensating Controls: An Impermanent Solution to an IT Compliance Gap | Tripwire.” *Www.tripwire.com*, www.tripwire.com/state-of-security/compensating-controls.

Boutin, Chad. “NIST Releases Version 2.0 of Landmark Cybersecurity Framework.” *NIST*, 26 Feb. 2024, www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.

Gargan, Richard. “Compensating Controls: How to Secure Legacy OT Systems.” *Netmaker.io*, 2024, www.netmaker.io/resources/compensating-controls-in-ot-systems.

HHS. “Summary of the HIPAA Security Rule.” *U.S. Department of Health and Human Services*, 30 Dec. 2024, www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

National Institute of Standards and Technology (NIST). “Security and Privacy Controls for Information Systems and Organizations.” *Csrc.nist.gov*, Sept. 2020, csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

Ponemon Institute. *Third Annual Benchmark Study on Patient Privacy & Data Security Sponsored by ID Experts Independently Conducted by Ponemon Institute LLC*. 2012.

Rupert, Jacque. “We Just Did a BIA and Gap Analysis… Now What? - Risk and Resilience Hub.” *Risk and Resilience Hub*, 15 June 2015, riskandresiliencehub.com/we-just-did-a-bia-and-gap-analysis-now-what/. Accessed 7 Aug. 2025.

Team 82. “The Importance of Compensating Controls in Cybersecurity.” *Claroty*, 6 Apr. 2023, claroty.com/blog/ot-icefall-vulnerabilities-underscore-the-importance-of-compensating-controls.

Wicks, Diana. “An Audit Checklist for Outsourcing a Performing Supplier.” *Small Business - Chron.com*, smallbusiness.chron.com/audit-checklist-outsourcing-performing-supplier-17764.html.