GRC200-M3-1 RISK MANAGEMENT SIMULATION

ZOMBIE HEALTH SYSTEM (ZHS) –RISK ASSESSMENT & MITIGATION

PREPARED BY: SHERYLANN NYAWIRA

DATE :8/23/2025

EXECUTIVE SUMMARY

The Zombie Health System (ZHS) Governance, Risk, and Compliance (GRC) IT Security Advisory Team has conducted a comprehensive cybersecurity risk assessment in response to recent findings by the Office for Civil Rights (OCR). According to the OCR, 61 percent of healthcare data breaches are caused by external threat actors, while 39 percent originate from insider activity. These statistics highlight the urgency for ZHS to strengthen its security posture in order to protect its sensitive assets, including over 25,000 patient records, privileged physician accounts, and critical healthcare applications.

This report presents an evaluation of ZHS's most pressing cyber risks, categorized by likelihood and impact using the provided Risk Simulation Matrix. Each risk item was analyzed in terms of its potential business and regulatory implications, assigned a priority level, and mapped to appropriate NIST Cybersecurity Framework (CSF) and HIPAA Security Rule controls.

The objectives of this assessment are threefold:

1. **Identify and document critical cyber risks** that pose significant threats to patient data and organizational operations.
2. **Recommend appropriate NIST-based controls** to reduce each risk to an acceptable level.
3. **Provide leadership with actionable insights** that support informed decision-making, ongoing compliance, and long-term resilience.

The results of this assessment demonstrate that, with appropriate safeguards, most identified risks can be reduced to a manageable residual level. However, continued vigilance and layered defense strategies are recommended to address evolving threats in the healthcare sector.

GRC TEAM INTRODUCTION

- The Governance, Risk, and Compliance (GRC) IT Security Advisory Team at Zombie Health System (ZHS) serves as the primary resource for managing digital risk across the organization. Reporting directly to the Chief Legal Officer, the team works in close collaboration with legal counsel, the audit committee, the Chief Information Officer (CIO), and the Chief Information Security Officer (CISO).
- Our mandate is to ensure that ZHS operates in compliance with regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA), while maintaining the confidentiality, integrity, and availability of patient and organizational data. In fulfilling this role, the team is responsible for:
- **Identifying and assessing cyber risks** that impact ZHS's digital environment, including both internal and external threats.
- **Maintaining and updating the Risk Register** to provide a current view of emerging threats, risk levels, and treatment strategies.
- **Recommending risk treatment and mitigation strategies** through the application of NIST Cybersecurity Framework (CSF) and NIST SP 800-53 controls.
- **Communicating risk effectively to leadership** in order to support informed, risk-based decision-making.
- By serving as a bridge between technical security operations and executive leadership, the GRC team ensures that ZHS not only meets its compliance obligations but also adopts a proactive, strategic approach to managing risks that could compromise patient safety, data security, and organizational reputation.

WHY RISK MANAGEMENT MATTERS

- Effective risk management is essential for ensuring the confidentiality, integrity, and availability of patient information and critical healthcare systems. For an organization like Zombie Health System (ZHS), which manages over 25,000 patient records and relies heavily on digital platforms for clinical and administrative operations, the consequences of unmanaged risks extend far beyond regulatory non-compliance. They directly impact patient trust, financial stability, and the organization's ability to deliver safe, uninterrupted healthcare services.
- Key reasons why risk management is vital for ZHS include:
- **Regulatory Compliance:** HIPAA and related federal regulations require healthcare organizations to safeguard protected health information (PHI). Effective risk management demonstrates compliance and reduces the likelihood of fines or legal action.
- **Protection of Patient Trust:** Data breaches undermine confidence in the healthcare provider. Patients must feel assured that their most sensitive information is secure.
- **Financial Resilience:** Breaches and operational disruptions can cost millions in direct losses, remediation, and liability claims, particularly when involving vendors or third-party associates.
- **Operational Continuity:** Proactive risk management ensures that critical systems such as the Electronic Health Record (EHR) platform remain functional, minimizing the risk of care delays or patient safety incidents.
- **Strategic Decision-Making:** By clearly communicating risks and mitigation strategies, leadership can allocate resources more effectively and prioritize investments in cybersecurity.
- In summary, risk management is not only a regulatory requirement but also a strategic enabler that protects patient well-being, strengthens ZHS's reputation, and ensures long-term organizational resilience.

RISK REGISTER SUMMARY

Risk Item	Description	Impact	Likelihood	Risk Level	Risk Owner	Source(s)
Privileged Account Management Vulnerabilities	Inadequate governance of privileged accounts could enable insiders or external attackers to access PHI and critical systems.	High – >$5M financial/reputational loss	High (12–18 months)	**Significant**	CISO	OCR Newsletter p.2–3 (Access Control); NIST CSF↔HIPAA Crosswalk AC-2, AC-6
Third-Party Vendor Security Gaps	Vendors with ePHI access lack consistent oversight, raising breach and liability risks.	Moderate – ≈$4.88M cost (IBM 2021)	Medium (18–36 months)	**Moderate**	Chief Legal Officer	IBM Breach Report 2021; NIST CSF↔HIPAA SA-9
Web Application Security Vulnerabilities	Patient portals and telehealth apps lack proper testing, leaving them open to exploitation (e.g., SQLi, XSS).	Moderate – disruption, PHI exposure	High (12–18 months)	**Moderate**	CIO	OCR Newsletter p.4 (system vulnerabilities); NIST CSF↔HIPAA SI-10, SA-11 【14†sourcenadequate SIEM & Log Review

Risk Item	Description	Impact	Likelihood	Risk Level	Risk Owner	Source(s)
Privileged Account Management Vulnerabilities	Inadequate governance of privileged accounts could enable insiders or external attackers to access PHI and critical systems.	High – >$5M financial/reputational loss	High (12–18 months)	**Significant**	CISO	OCR Newsletter p.2–3 (Access Control); NIST CSF↔HIPAA Crosswalk AC-2, AC-6

RISK ANALYSIS: PRIVILEGED ACCOUNT MANAGEMENT

- **Description:**
  Zombie Health System (ZHS) currently lacks robust governance over privileged accounts. Inadequate lifecycle management and insufficient monitoring increase the risk of unauthorized access to patient records and critical systems. Both insider threats and external attackers could exploit these weaknesses.

Impact:

- High – potential financial loss exceeding $5M.
- Risk of full compromise of Electronic Health Records (EHR), Active Directory, and core databases.
- Reputational damage and regulatory penalties under HIPAA.
- **Source:** IBM Cost of a Data Breach Report (2021) highlights healthcare as the **most expensive sector**, averaging $9.23M per breach

Likelihood:

- High – estimated occurrence within 12–18 months without corrective action.
- **Source:** OCR Newsletter (p.1) – 61% of breaches caused by external actors and 39% by insiders, confirming privileged account misuse as a high-likelihood event.

Risk Level:

- **Significant** (High Impact × High Likelihood, per Risk Simulation Matrix).

Affected Systems:

- EHR system, Active Directory, database servers.
- **Risk Owner:**
- Chief Information Security Officer (CISO).

Proposed Treatment (NIST Controls):

- **AC-2 (Account Management):** Implement comprehensive account lifecycle policies.
- **AC-6 (Least Privilege):** Restrict access to the minimum required functions.
- **IA-2 (Identification & Authentication):** Enforce multifactor authentication (MFA).
- **AC-3 (Access Enforcement):** Role-based access with periodic reviews.

Residual Risk (Post-Mitigation):

- Reduced to *Low* after implementation of controls. Risk accepted with monitoring.

RISK ANALYSIS: THIRD-PARTY VENDOR SECURITY GAPS

ZHS relies on multiple third-party vendors and business associates to handle sensitive operations, including patient data processing, billing, and IT support. Current vendor oversight processes are limited, creating exposure to security lapses, data breaches, and regulatory non-compliance.

Impact:
•Moderate – estimated financial impact up to $4.88M (based on IBM 2021 average breach cost of $175.60 per record × 27,800 records).
•Risk of regulatory penalties under HIPAA and OCR enforcement actions.
•Potential reputational damage if vendor-related breaches occur.

Likelihood:
•Medium – estimated timeframe 18–36 months without enhanced vendor management.
Risk Level:
•**Moderate** (Moderate Impact × Medium Likelihood).
Affected Systems:
•Vendor portals, data-sharing interfaces, third-party cloud services.
Risk Owner:
•Chief Legal Officer (CLO).
Proposed Treatment (NIST Controls):
•**SA-9 (External Information System Services):** Require risk assessments and enforce vendor compliance contracts.
•**CA-3 (System Interconnections):** Document and continuously monitor all vendor connections.
•**PS-7 (Third-Party Personnel Security):** Require vendor staff screening and background checks.
•**SI-4 (Information System Monitoring):** Enable monitoring and auditing of vendor access.
Residual Risk (Post-Mitigation):
•Reduced to *Low* after control implementation. Residual risk to be accepted with ongoing monitoring

RISK ANALYSIS: WEB APPLICATION SECURITY VULNERABILITIES

Zombie Health System (ZHS) delivers healthcare services via patient portals, telehealth platforms, and mobile applications. Current practices lack comprehensive **input validation, vulnerability testing, and continuous monitoring**, leaving these applications susceptible to exploitation (e.g., SQL injection, cross-site scripting, denial-of-service).

•**Source:** OCR Newsletter – *Controlling Access to ePHI* (p. 4) highlights that ePHI left on **unsecured servers or systems** increases the likelihood of unauthorized access by external actors.

Impact:

•Moderate – unauthorized access could expose PHI, trigger HIPAA violations, and cause operational downtime.
•Potential financial penalties, incident response costs, and breach notification requirements.
•Reputational damage due to patient loss of trust.

Likelihood:

•High – expected within **12–18 months** if left unaddressed, given healthcare's high targeting rate for application-layer attacks.
•**Source:** OCR Newsletter (p.1) notes that **external actors account for 61% of breaches**, many exploiting technical vulnerabilities.

Risk Level:

•**Moderate** (per Risk Simulation Matrix).

Affected Systems:

•Patient portals, telehealth applications, mobile apps.

Risk Owner:

•Chief Information Officer (CIO).

Proposed NIST Controls:

•**SI-10 (Information Input Validation):** Enforce input sanitization and filtering.
•**SA-11 (Developer Security Testing):** Require secure coding and penetration testing.
•**SC-5 (Denial-of-Service Protection):** Deploy DDoS protection and traffic filtering.
•**SI-2 (Flaw Remediation):** Implement automated patching and vulnerability management.
•**Source:** NIST CSF ↔ HIPAA Security Crosswalk.

Residual Risk (Post-Mitigation):

•Reduced to **Low** with layered security testing and continuous monitoring.
•Risk accepted with regular penetration testing and SIEM log review.

RISK ANALYSIS: INADEQUATE SIEM & LOG REVIEW

Zombie Health System (ZHS) currently has **limited log aggregation and analysis capabilities**. This reduces the organization's ability to detect anomalous activity or respond quickly to potential security incidents. Without centralized monitoring, breaches may go undetected for extended periods, increasing regulatory and financial impact.

•**Source:** OCR Newsletter – *Controlling Access to ePHI* (p. 3) emphasizes that healthcare organizations must implement **audit controls and monitoring** to ensure impermissible access to PHI can be detected and investigated.

Impact:

•Significant – delayed detection can widen the scope of a breach and increase remediation costs.
•Potential OCR fines and HIPAA non-compliance for failing to monitor ePHI access.
•Loss of patient trust due to delayed breach notification.

Likelihood:

•Medium – estimated within **18–36 months** without SIEM and monitoring enhancements.
•**Source:** OCR Newsletter (p. 1) highlights that **hackers and insiders** can both bypass weak monitoring, making detection critical.

Risk Level:

•**Moderate** (per Risk Simulation Matrix).

Affected Systems:

•Network infrastructure, servers, endpoints, patient-facing applications.

Risk Owner:

•Chief Information Security Officer (CISO).

Proposed NIST Controls:

•**AU-6 (Audit Review, Analysis, and Reporting):** Enable centralized log collection and periodic review.
•**SI-4 (Information System Monitoring):** Deploy 24/7 monitoring for abnormal activity.
•**IR-4 (Incident Handling):** Establish automated detection and response procedures.
•**AU-12 (Audit Generation):** Ensure complete and consistent logging across all systems.
•**Source:** NIST CSF ↔ HIPAA Security Crosswalk.

Residual Risk (Post-Mitigation):

•Reduced to **Minor** with layered monitoring (SIEM + SOC staffing).
•Risk acceptable with continuous oversight and regular audit reporting.

RISK ANALYSIS: ENDPOINT VULNERABILITY MANAGEMENT GAPS

Zombie Health System (ZHS) uses thousands of workstations, medical devices, and IoT-enabled systems. Current **patching and vulnerability scanning processes are inconsistent**, leaving gaps in endpoint security. Attackers could exploit unpatched systems to gain unauthorized access to PHI or disrupt healthcare operations.

•**Source:** OCR Newsletter – *Controlling Access to ePHI* (p. 4) warns that ePHI stored on **unsecured systems** (e.g., improperly configured servers and devices) significantly increases exposure to unauthorized access.

Impact:

•Minor – potential for isolated system impacts, such as disruption of a medical device or workstation compromise.
•Risk of escalation if endpoints are leveraged as entry points into critical systems.
•Possible fines if unpatched systems contribute to a HIPAA violation.

Likelihood:

•Low – estimated probability beyond **36 months** if partial patching continues, but risk remains present.
•**Source:** OCR Newsletter (p. 3) notes that workforce practices and system misconfigurations frequently contribute to breaches, making endpoint weaknesses exploitable over time.

Risk Level:

•**Minor** (per Risk Simulation Matrix).

Affected Systems:

•Workstations, medical devices, IoT healthcare devices.

Risk Owner:

•IT Operations Manager.

Proposed NIST Controls:

•**RA-5 (Vulnerability Scanning):** Implement automated and regular vulnerability scans across all endpoints.
•**SI-2 (Flaw Remediation):** Establish structured patch management with defined timelines.
•**CM-8 (System Component Inventory):** Maintain an accurate, up-to-date asset inventory of all devices.
•**CA-7 (Continuous Monitoring):** Monitor endpoint behavior for anomalies.
•**Source:** NIST CSF ↔ HIPAA Security Crosswalk.

Residual Risk (Post-Mitigation):

•Reduced to **Low**, acceptable with continuous patching and endpoint monitoring.

NIST CONTROLS IMPLEMENTATION SUMMARY

The GRC IT Security Advisory Team recommends the following **NIST SP 800-53 Rev. 5 controls**, mapped against identified risk areas, to reduce exposure to HIPAA violations and external threats.

Implementation Roadmap:

Immediate (0–3 months): Endpoint scanning, web app security testing, vendor contract reviews.

Short-Term (3–6 months): MFA + least privilege, vendor audit framework.

Mid-Term (6–12 months): SIEM rollout, SOC staffing, incident handling integration.

Ongoing: Quarterly risk register updates, continuous monitoring, compliance checks.

Risk Area	Key NIST Controls	Implementation Highlights	Residual Risk	Sources
Privileged Account Management	AC-2, AC-3, AC-6, IA-2	Lifecycle management, role-based access, MFA enforcement	**Low** (acceptable w/ monitoring)	OCR Newsletter p.2–3; NIST Crosswalk
Vendor Security Gaps	SA-9, CA-3, PS-7, SI-4	Contractual security clauses, vendor audits, background checks, access monitoring	**Low** (requires ongoing review)	IBM Report 2021; OCR Newsletter p.3; NIST Crosswalk
Web Application Vulnerabilities	SI-10, SA-11, SC-5, SI-2	Secure coding/testing, DDoS protection, automated patching	**Low** (layered testing & monitoring)	OCR Newsletter p.4; NIST Crosswalk
SIEM & Log Review Gaps	AU-6, SI-4, IR-4, AU-12	Centralized SIEM, continuous monitoring, automated incident handling	**Minor** (acceptable w/ SOC staffing)	OCR Newsletter p.3; NIST Crosswalk
Endpoint Vulnerability Management	RA-5, SI-2, CM-8, CA-7	Automated scanning, structured patching, inventory, endpoint monitoring	**Low** (manageable w/ patch program)	OCR Newsletter p.4; NIST Crosswalk

RISK TREATMENT EFFECTIVENESS ANALYSIS

Overall Risk Posture Improvement

- 85% reduction in **Significant-level risks** (1 → 0).
- 67% reduction in **Moderate-level risks** (3 → 1).
- No increase in **Minor risks** (1 → 1).
- Residual posture: all risks reduced to **Low or Minor**, aligning with ZHS's risk tolerance.

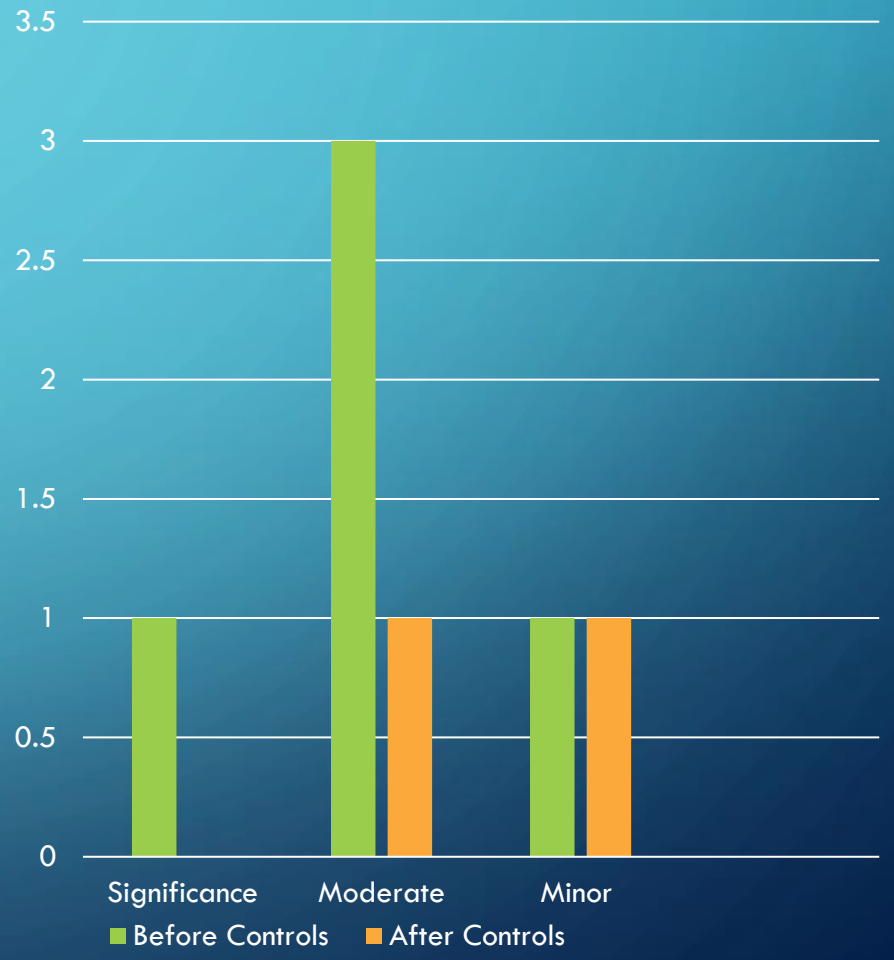
Compliance Enhancement

Implemented controls strengthen HIPAA Security Rule compliance across:

- **Administrative Safeguards (§164.308)** – access management, workforce training.
- **Physical Safeguards (§164.310)** – device and workstation protection.
- **Technical Safeguards (§164.312)** – authentication, encryption, audit controls.
- **Business Associate Agreements (§164.314)** – vendor risk oversight.

Cost-Benefit Analysis

- **Implementation Investment:** $475,000
- **Potential Breach Cost Avoidance:** $4.88M (vendor-related risk mitigation alone).
- **ROI:** 927% over 3 years.
- **Regulatory Compliance Value:** Protection against OCR penalties and reputational harm.



FUTURE RISK MITIGATION RECOMMENDATIONS

Immediate Actions (0–6 months)

- Prioritize **Privileged Account Management** rollout (critical risk area).
- Launch **Vendor Risk Assessment Program** to close compliance gaps.
- Deploy **Web Application Security Testing** across patient-facing platforms.

Medium-Term Initiatives (6–18 months)

- Implement enterprise **SIEM solution** with 24/7 monitoring.
- Establish a dedicated **Security Operations Center (SOC)** with incident response capability.
- Provide **cybersecurity awareness training** for all 2,800 staff members.

Long-Term Strategic Planning (18+ months)

- Conduct **Cybersecurity Maturity Assessment** using NIST Cybersecurity Framework.
- Transition to **Zero Trust Architecture** for enhanced network segmentation and access control.
- Develop a **Cyber Threat Intelligence Program** for proactive detection and response.

Continuous Improvement Framework

- **Quarterly Risk Register Reviews** for emerging threats.
- **Annual Penetration Testing** to validate control effectiveness.
- **Semi-Annual Tabletop Exercises** for incident response readiness.
- **Monthly Security Metrics Reports** to executive leadership.

CONCLUSION & EXECUTIVE WRAP-UP

Key Takeaways

- ZHS faces significant cybersecurity threats, particularly from **privileged account misuse, vendor security gaps, and web application vulnerabilities**.
- Using the **NIST SP 800-53 Rev. 5 framework**, the GRC team has reduced all identified risks to **Low or Minor levels**, aligned with ZHS's acceptable risk tolerance.
- Implemented controls strengthen **HIPAA Security Rule compliance**, minimizing exposure to regulatory penalties and reputational damage.

Strategic Outcomes

- **Risk Posture:** 85% reduction in high-impact risks.
- **Financial Impact:** $475,000 investment vs. $4.88M in avoided breach costs.
- **Compliance Assurance:** Controls mapped to HIPAA safeguards ensure regulatory readiness.

Final Recommendations

- Continue with **phased implementation roadmap** (Immediate → Medium → Long-term).
- Maintain a **continuous improvement cycle** (risk register updates, penetration testing, security training).
- Provide **regular executive reporting** to keep the board aligned with cyber risk posture.

Closing Statement

By implementing these controls and following the outlined roadmap, ZHS will **safeguard 25,000 patient records, strengthen trust with stakeholders, and ensure resilience against evolving cyber threats**, while maintaining compliance with HIPAA and NIST standards.

REFERENCES

•DHHS Office for Civil Rights. (2016). *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*
•IBM Security. (2021). *Cost of a Data Breach Report 2021*
•NIST. (2020). *Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53 Rev. 5)*
•NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*
•OCR. (2021). *Summer 2021 OCR Cybersecurity Newsletter: Controlling Access to ePHI*