Nexus
GRC Solutions

Zombie_health_system_report

Table of Contents

GRC Team Introduction

We are the Nexus GRC Solutions team that recently engaged to assist Zombie Health System in managing and mitigating risks while ensuring regulatory compliance. Our team consists of experienced professionals with diverse expertise in healthcare risk management, regulatory affairs, cybersecurity, compliance auditing, and process improvement.

Our key skillsets include:

- Risk Assessment and Analysis: Identifying and evaluating clinical, operational, financial, and technological risks specific to healthcare environments.
- Regulatory Compliance: Deep knowledge of healthcare laws and standards such as HIPAA, patient safety regulations, and industry best practices.
- Cybersecurity and Data Protection: Expertise in safeguarding sensitive patient and organizational data against evolving cyber threats.
- Policy Development and Implementation: Crafting clear, actionable policies and controls to manage risks and ensure consistent compliance across departments.
- Risk Communication and Stakeholder Engagement: Facilitating clear communication of risk findings and mitigation strategies to executive leadership, clinical teams, and external stakeholders for informed decision-making.
- Process Optimization and Continuous Improvement: Applying process improvement methodologies such as Lean and Six Sigma to streamline risk management workflows and enhance operational resilience.

GRC Team Staff

Name	Role	Expertise	Contact
Paul Mwaniki	Lead Risk Manager	Healthcare Risk Assessment, Clinical Safety	paul.mwaniki@nexusgrc.com
Markus Mwangi	Regulatory Compliance Officer	HIPAA, Healthcare Regulations	markus.mwangi@nexusgrc.com
David Opiyo	Cybersecurity Specialist	Data Protection, Cyber Threat Mitigation	david.opiyo@nexusgrc.com
Lear Wairimu	Compliance Auditor	Process Auditing, Policy Enforcement	lear.wairimu@nexusgrc.com
Sophia wangeci	Process Improvement Analyst	Lean Six Sigma, Operational Resilience	sophia.wangeci@nexusgrc.com

Risk Management Summary

The risk management process is a systematic approach used to identify, assess, and mitigate risks that could negatively impact an organization’s operations, assets, or stakeholders. This structured framework helps healthcare organizations manage uncertainty and maintain a safe, compliant, and efficient operating environment. In healthcare, this process focuses particularly on preventing harm to patients, staff, and the facility by proactively addressing potential threats and vulnerabilities. The typical steps include:

- Risk Identification: Recognizing potential hazards and risks within the healthcare environment.
- Risk Analysis: Evaluating the likelihood and consequences of identified risks.
- Risk Evaluation: Prioritizing risks by severity and organizational impact.
- Risk Treatment: Implementing measures to reduce or eliminate risks.
- Monitoring and Review: Continuously tracking risk status and the effectiveness of treatments to adjust as needed.

Value of the Risk Management Process to Zombie Health System

For Zombie Health System, an effective risk management process is critically valuable because it:

- Protects Patient Safety: By identifying and addressing clinical and operational risks, it ensures safer care delivery and reduces adverse events.
- Safeguards Data and Compliance: Helps prevent data breaches and ensures adherence to healthcare regulations, protecting patient privacy and legal standing.
- Enhances Operational Resilience: Anticipates and mitigates challenges that could disrupt services, maintaining business continuity.
- Reduces Financial Losses: Minimizes risks that could lead to costly litigation, penalties, or operational downtime, preserving financial stability.
- Facilitates Informed Decision-Making: Provides valuable risk insights that support strategic planning and resource allocation.
- Boosts Stakeholder Confidence: Demonstrates commitment to safety and compliance, fostering trust among patients, staff, and regulatory bodies.

Risk Register Data

Risk Register Summary

The primary risks identified revolve around unauthorized access and misuse of electronic protected health information (ePHI) due to weaknesses in identity and access management, including the use of shared user credentials and insufficient access authorization policies. Vendor management risks highlight potential data breaches through third-party service providers, which could lead to significant liability given the volume of records involved. Access control vulnerabilities include the absence of encryption, ineffective emergency access procedures, and the lack of automatic logoff mechanisms, all of which increase exposure to unauthorized data access. Insufficient security information and event management (SIEM) and log review capabilities hamper timely detection and investigation of security incidents. Web application security risks stem from exploitable vulnerabilities, and poor vulnerability management practices such as unpatched systems further expose the organization to cyber threats.

Identity Access Management

- Unauthorized access via shared user credentials (lack of unique user IDs).
- Inadequate access authorization policies.
- Lack of periodic access review/modification processes.
- Insider threats from workforce members accessing ePHI beyond roles.

Vendor Management (Contract Liability Risk)

- Data breach caused by third-party vendors with access to ePHI.
- Inadequate contractual clauses regarding data protection and breach liabilities.
- Potential regulatory fines based on number of breached records (estimate 27,800 records x cost per record).

Access Controls

- Absence or failure of encryption and decryption of ePHI.
- Lack of or ineffective emergency access procedures.
- Non-implementation of automatic logoff on inactive sessions.
- Poor network segmentation and firewalling enabling lateral movement by attackers.

SIEM and Log Review

- Inadequate or lack of audit controls and logging.
- Delayed or ineffective review of security logs and alerts.
- Using shared user IDs impeding accountability and forensic investigation.

Web Application Security

- Vulnerabilities in healthcare applications exposing ePHI.
- Insufficient input validation and access control on application layers.

Vulnerability Management

- Unpatched systems and applications with known vulnerabilities.
- Absence of regular vulnerability scanning and penetration testing.

Risk ID	Risk Category	Description	Priority	Risk Owner	Dependent Systems	Mitigation Summary
1	Identity Access Management	Unauthorized access due to shared credentials, lack of unique IDs, and insufficient authorization	High	IT Security Manager	User accounts, Access Control Systems	Enforce unique IDs, implement role-based access, periodic reviews
2	Vendor Management	Data breach via third-party vendors with inadequate data protection clauses	High	Vendor Manager	Third-party systems	Strengthen vendor contracts, conduct regular audits
3	Access Controls	Lack of encryption, emergency access procedures, and auto logoff increasing unauthorized access	High	IT Operations Lead	EHR systems, Network devices	Deploy encryption, update access policies, implement auto logoff
4	SIEM and Log Review	Ineffective auditing, delayed log review, and shared IDs hampering incident detection	Medium-High	Security Operations	SIEM, Logging Infrastructure	Enhance logging, implement real-time monitoring, assign accountability

Risk ID	Risk Category	Description	Priority	Risk Owner	Dependent Systems	Mitigation Summary
5	Web Application Security	Vulnerabilities in healthcare apps due to poor input validation and access controls	Medium	Application Security	Healthcare applications	Apply security testing, enforce secure coding standards
6	Vulnerability Management	Unpatched systems, absence of regular vulnerability scans and penetration testing	Medium	Patch Management Team	All IT systems	Schedule regular patching, automated vulnerability scans

Risk Register Analysis

Risk Register Summary

To mitigate these risks, NIST controls focus on strengthening identity and access management by implementing unique user identification, enforcing least privilege access, and regularly reviewing access rights, which enhances accountability and minimizes insider threats. Vendor management controls require rigorous risk assessments and contractual protections to manage third-party risks effectively. Access control measures emphasize encryption of ePHI, robust emergency access procedures, and session timeout capabilities to protect data confidentiality and ensure secure access during emergencies. SIEM-related controls improve audit logging, prompt log analysis, and incident reporting to bolster detection and response capabilities. Web application security is enhanced through secure development practices and continuous integrity monitoring, while vulnerability management controls mandate regular scanning and timely patching to reduce exploitable weaknesses. Collectively, these controls substantially reduce the likelihood and impact of cybersecurity incidents, thereby bringing risks down to an acceptable level.

Risk Item	**Identified Risk**	**NIST Control(s) Suggested**	**Impact on Risk**
Identity Access Management	Shared IDs, unauthorized access, insider threats	AC-2 (Account Management), AC-6 (Least Privilege), PS-4 (Personnel Termination), IA-2 (Identification and Authentication)	Reduce unauthorized access, improve accountability
Vendor Management	Third-party breaches, liability exposure	SA-9 (External Information System Services), SA-12 (Supply Chain Protection), RA-3 (Risk Assessment)	Lower risk from vendor weaknesses, contract enforcement
Access Controls	Lack of encryption, emergency access failures	SC-12 (Cryptographic Key Establishment), SC-13 (Cryptographic Protection), AC-17 (Remote Access), AC-11 (Session Lock)	Improve data confidentiality and emergency handling
SIEM and Log Review	Inadequate logging and audit trails	AU-2 (Audit Events), AU-6 (Audit Review, Analysis, and Reporting), IR-6 (Incident Reporting)	Strengthen detection and accountability

Risk Item	Identified Risk	NIST Control(s) Suggested	Impact on Risk
Web App Security	Application vulnerabilities	SA-11 (Developer Security Testing), SI-7 (Software, Firmware, and Information Integrity), SA-10 (Developer Configuration Management)	Reduce exploit and vulnerability risks
Vulnerability Management	Unpatched systems	RA-5 (Vulnerability Scanning), SI-2 (Flaw Remediation)	Minimize exploitation opportunities

Presentation Of Risks

summary of risks

The organization faces a high overall cybersecurity risk focused on protecting ePHI confidentiality and integrity.

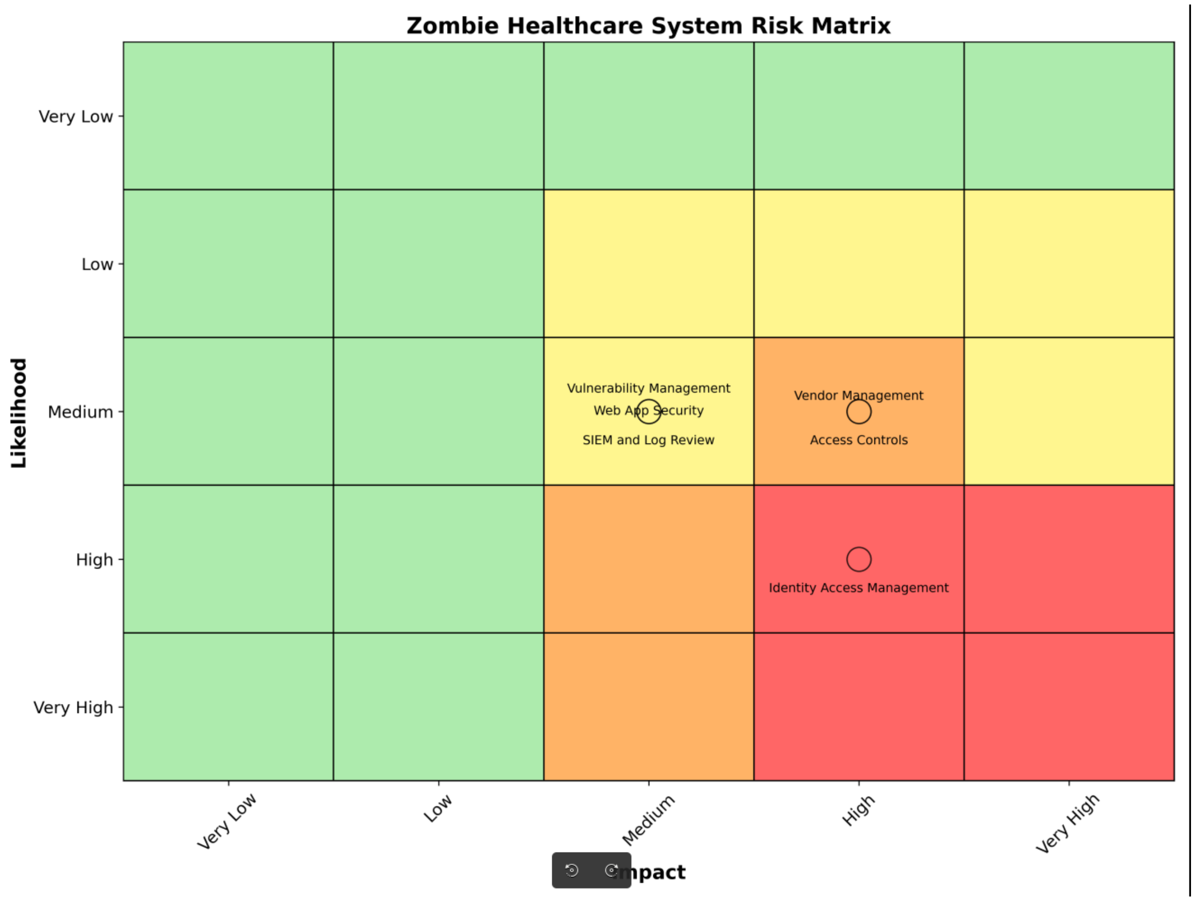
Identity and access management, coupled with vendor security, represent priority risk domains requiring immediate intervention.

Mitigating these risks with robust NIST controls will substantially reduce potential breaches and regulatory fines.

Proactive governance, continuous monitoring, and a culture of security awareness are vital to sustained risk reduction.

Executive leadership commitment is critical to allocate resources and champion security initiatives.

Risk matrix



Conlcusion And Findings

To deliver a more robust and actionable GRC recommendation tailored specifically for the healthcare cybersecurity risks identified, we need to focus on practical, integrated strategies that drive measurable risk reduction and organizational resilience:

Cultural and Operational Integration:

- Strengthen insider threat programs with tailored training sessions, role-based access review protocols, and whistleblower channels.
- Embed security and privacy by design in all healthcare IT developments and process changes, supported by secure software development lifecycle (SDLC) practices, including threat modeling and code reviews.
- Coordinate cross-departmental drills simulating ransomware or breach incidents involving remote teleworking scenarios, aligning with emergency access procedures.

Technology Enablement:

- Deploy identity governance and administration (IGA) systems that enforce unique user IDs, least privilege, and automated provisioning/deprovisioning.
- Invest in advanced SIEM and UEBA (User and Entity Behavior Analytics) solutions for early detection of unusual access patterns.
- Integrate encryption solutions that comply with NIST SP 800-111 standards for data at rest and in transit, covering mobile and cloud environments.

Future-proofing and Continuous Improvement:

- Conduct quarterly risk reassessments incorporating latest threat intelligence and incident lessons learned.
- Establish KPIs and KRIs related to access violations, encryption coverage, incident response times, and audit compliance rates.
- Create a formal feedback loop that feeds risk posture insights back into governance and strategic planning.

Source List

Key GRC Healthcare Resources List

1. Microminder – GRC for Healthcare Cybersecurity https://www.micromindercs.com/blog/grc-for-healthcare-cybersecurity Step-by-step framework tailored for healthcare cybersecurity risk management and compliance.
2. Healthcare Sector Cybersecurity Framework Implementation Guide (CISA & HITRUST) https://www.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf Comprehensive guide for implementing the NIST Cybersecurity Framework in healthcare, aligned with HITRUST and HIPAA.
3. MetricStream – Cybersecurity GRC Guide https://www.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf Practical insights on aligning cybersecurity risk management with business goals and regulatory compliance.
4. Riskonnect – GRC Implementation Roadmap https://www.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf Structured approach for GRC program implementation focused on governance and risk prioritization.
5. Scrut – Critical Healthcare Cybersecurity Regulations and Frameworks https://www.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf Overview of key regulations and frameworks such as HIPAA, NIST, HITRUST relevant to healthcare cybersecurity.
6. Steel Patriot Partners – GRC Software for Healthcare Cybersecurity https://www.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf Guide on leveraging GRC software solutions to streamline compliance and risk visibility in healthcare.
7. Department of Health (DoH) – Healthcare Cybersecurity Workforce Guidelines https://www.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf Policy and workforce strategy guidelines to support cybersecurity standards and compliance in healthcare.