NIST Risk Assessment
Zombie Health System (ZHS)

Business Confidential

Date: 10/29/2023
Project: 897-20
Version 1.0

Table of Contents

INTRODUCTION

Purpose Of The Risk Management Plan

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring and controlling, and reporting risks. This Risk Management Plan defines how risks associated with the *Zombie Health Systems* project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks by the Risk Manager and/or Risk Management Team.

The role of the GRC IT Security Advisors is to provide guidance on governance, risk, and compliance in the digital environment. Risks related to IT systems or applications must be identified and documented based on the methodology in NIST SP 800-53 Control Catalog..

RISK MANAGEMENT PROCEDURE

PROCESS

The project manager working with the project team and project sponsors will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. Risks will be identified as early as possible in the project so as to minimize their impact. The steps for accomplishing this are outlined in the following sections.

Role	Responsibilities
Business SME (BSME)	The BSME assists in identifying and determining the context, consequence, impact, timing, and priority of the risk.
Risk Manager or Project Manager (PM)	The Risk Manager or PM is a member of the Integrated Project Team (IPT). The Risk Manager or PM determines if the Risk is unique, identifies risk interdependencies across projects, verifies if risk is internal or external to the project, assigns risk classification and tracking number. During the life of the project, they continually monitor the projects for potential risks.
Integrated Project Team	The IPT is responsible for identifying the risks, the dependencies of the risk within the project, the context and consequence of the risk. They are also responsible for determining the impact, timing, and priority of the risk as well as formulating the risk statements.
Risk Owner(s)	The risk owner determines which risks require mitigation and contingency plans, he/she generates the risk mitigation and contingency strategies and performs a cost benefit analysis of the proposed strategies. The risk owner is responsible for monitoring and controlling and updating the status of the risk throughout the project lifecycle. The risk owner can be a member of the project team.
Other Key Stakeholders	The other stakeholders assist in identifying and determining the context, consequence, impact, timing, and priority of the risk.

RISK IDENTIFICATION

Risk identification will involve the project team, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope, schedule, cost, or quality. Careful attention will be given to the project deliverables, assumptions, constraints, cost/effort estimates, resource plan, and other key project documents.

METHODS FOR RISK IDENTIFICATION

A *Risk Register* will be used as a Risk Management Tool to fulfill regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g., nature of their risk, reference and owner, mitigation measures. It can be displayed as a scatter plot or as a table.

RISK ANALYSIS

A Risk Assessment determines possible mishaps, their likelihoods and consequences, and their tolerances for each event. This assessment aims to identify and manage risks effectively. For Zombie Healthcare Systems it is critical to protect patient records and the board's directives. All risks identified will be assessed to identify the range of possible project outcomes. Risks will be prioritized by their level of importance.

Risk Management Actions		
Considerable Risk Management Required	**Risk management Required**	**Extensive Risk Management Essential/Insurance**
Risk Acceptance may be possible with monitoring	**Risk Management Applied**	**Risk Management Required**
Accept Risk	**Risk Acceptance with monitoring**	**Risk Management Applied**
LOW **> 36 months**	**MEDIUM** **18-36 months**	**HIGH** **12-18 months**

RISK ANALYSIS

Impact

Significant

- Financial loss > $5m
- Stakeholder faith impacted and lasts >18 months
- Isolated or multiple loss of revenue/assets
- Multiple events of fine, fraud, legal action
- Complete system crash with loss of critical data
- Inability to recruit, retain staff to operate
- Labor disruption that impacts profitability

Moderate

- Financial loss < $5m
- Stakeholder faith impacted and lasts 6-12 months
- Significant loss of revenue/assets
- Non-related incidents of fine, fraud, legal action
- System crash during a peak period
- Difficulty to recruit and retain staff
- Labor disruption that impacts operations of any duration

Minor

- Financial loss < $500,000
- Stakeholder faith impacted and lasts < 6 months
- Isolated loss of revenue/asset
- Single threat of fine, fraud, legal action
- System offline or failure during non-peak hours
- Slight impact to operational staff
- Labor disruption of insignificance

RISK ASSESSMENT

The following **NIST Risk Assessment** is in relation to all identified risk register items found at: RISK REGISTER ZHS

The NIST SP 800-53 controls in discussion can be found in full detail at:
NIST Control Catalog

Vendor Management - HIGH RISK

A vendor breach could lead to the exposure of protected health information (PHI) and financial data. It is important for vendors to uphold security standards, as any breach could deem to be extremely detrimental.

ZHS should regularly audit its vendors to make sure security is up to standard protocals.

NIST SP 800-53 AC-2 (Vendor Management) offers controls to be put in place:

- Require vendors to sign a vendor security agreement (VSA) that outlines their security obligations.
- Conduct vendor risk assessments to evaluate the security posture of vendors.
- Implement vendor security monitoring to detect and respond to security incidents involving vendors.

Identity and Access Management (IAM) - MEDIUM RISK

Multi-factor authentication should be implemented for all users. Single factor authentication is vulnerable to theft (phishing, man in the middle, social engineering, etc.) and forgery (brute force attacks, dictionary attacks, etc.) Multifactor authentication requires additional means of authentication other than a password for verifying a user's identity. The authentication process requires a user to provide a second different factor, "...usually either a security token or a biometric factor, such as a fingerprint or a facial scan" ("two-factor authentication").

RISK ASSESSMENT

NIST SP 800-53 AC-1 (Access Control) offers recommendations. The following are controls ZHS might put in place:

- Require MFA for all privileged accounts, such as those used by system administrators and medical professionals.
- Implement MFA for all remote access, such as VPNs and remote desktop connections.
- Educate users about MFA and how to use it effectively.

Healthcare organizations need to keep on top of access rights and ensure that permissions are appropriate to roles and responsibilities, with strong identity and access management, especially for privileged accounts.

NIST SP 800-53 AC-6 provides the principle of **Least privilege**, "...allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks."

A **zero-trust** approach assumes that the network has been compromised, and ensures that if there is a security breach, an attacker does not have free rein over everything inside the network perimeter. Zero trust involves a, "...constant process of authentication, authorization, and validation before access is granted to applications and data" ("Editorial: The Importance").

There is no doubt that zero trust is the future of healthcare security and can prevent malicious actors from gaining access to healthcare networks and data and limit the harm that can be caused when attacks succeed; however, adoption of zero trust has been slow in the healthcare industry.

Web APP Security - MEDIUM RISK

As mentioned in the press release from Outpost 24, " A significant 90% of web applications used by US healthcare operators are highly susceptible to attack or vulnerability exposure" ("Press Release"). As a result, these applications become vulnerable to injection attacks like cross site scripting (XSS) and SQL injection (SQLI), path traversal, local file inclusion, DDOS attacks, cross site request forgery (CSRF) and XML external entity (XXE).

NIST SP 800-53AT-2(4) (Anomalous System Behavior) deems it essential to perform **application level monitoring and auditing** of Web connections to strengthen web application security standards and lower vulnerability exposure.

RISK ASSESSMENT

SIEM and Log Review - LOW RISK

Many healthcare organizations discover their systems have been breached, "...several weeks or months after the network has been compromised, with the intrusion only detected when ransomware is used to encrypt files" ("Editorial: The Importance").

Upholding a **strong SIEM and log review system** will significantly reduce the impact of any potential breach or harm to a system. By sending logs to a SIEM system for collection and analysis appropriate action can be taken right away.

NIST SP 800-53 AC-6 (SIEM) offers potential controls to be put in place:

- Collect logs from all systems and networks.
- Implement real-time log analysis to detect suspicious activity.
- Implement automated response to security incidents.

Residual Risk

The residual risk for each associated item will be measured after the corresponding NIST control has been put in place. If the risk is still unacceptable additional controls may need to be put in place.

Recommendations:

As a measure of best practice it is important to **educate staff** about the importance of security. This education will prevent many security incidents from happening while **continuous monitoring** will allow security incidents to be addressed quickly

SUMMARY

This risk assessment identifies key risks to Zombie Health System (ZHS):

- **Vendor Management Liability Risk** A vendor breach could lead to the exposure of protected health information (PHI) and financial data.
- **Identity and Access Management (IAM)** An unauthorized user could gain access to ZHS systems and data.
- **Web App Security** A significant amount of web applications used by US healthcare operator are highly susceptible to attack or vulnerability exposure
- **SIEM and Log Review** SIEM and log review systems could fail to detect and respond to security incidents in a timely manner.

ZHS can mitigate these risks by implementing the following NIST controls:

- **Vendor Management Liability Risk:** Require vendors to sign a vendor security agreement , conduct vendor risk assessments, and implement vendor security monitoring.
- **Web App Security:** Perform application level monitoring and auditing of Web connections
- **Identity and Access Management (IAM):** Implement multi-factor authentication for all users, require MFA for all privileged accounts and remote access, and educate users about MFA. Implement principle of least privilege, adopt zero trust
- **SIEM and Log Review** Collect logs from all systems and networks, implement real-time log analysis, and implement automated responses to security incidents.

Conclusion

Zombie Health System can greatly diminish its overall risk to security breaches by adhering to the NIST SP 800-53 controls listed above. Implementation of these controls will help protect the security of all those affected whether that be customers, employees, or members in management positions. It is important to educate all employees about the dangers of security breaches as well as overall best practices. Placing IT security as a necessity will protect from the dangers of future attacks.

Works Cited

"Editorial: The Importance of Identity and Access Management (IAM) in Healthcare." *The HIPAA Journal*, www.hipaajournal.com/identity-access-management-iam-healthcare/#:~:text=Identity%20and%20access%20management%20in,are%20in%20place%20to%20prevent.

"Press Release: America's top healthcare providers run vulnerable web apps." *Outpost24*, outpost24.com/blog/top-healthcare-providers-run-vulnerable-web-apps/.

"two-factor authentication (2FA)." *Tech Target*, www.techtarget.com/searchsecurity/definition/two-factor-authentication?Offer=abMeterCharCount_ctrl#:~:text=Two%2Dfactor%20authentication%20methods%20rely,a%20fingerprint%20or%20facial%20scan.