AUDIT REPORT

Presented To
GANESH BHUSAL

Presented By
AVISHEK DHAKAL

Audit Report

Avishek Dhakal (CU ID:12981148 | Student ID: 220064)

ST6050CEM Security Audit and Monitoring

Ganesh Bhusal

Aug17, 2024

Table of Contents

Table of Figure

Figure **page no.**

Introduction

The Chief Information Security Officer (CISO) in the company is like a parent who oversees everything that concerns the security of the company. This report presents the findings and recommendations from the external audit conducted for Zenith Solutions; a software development firm based in Nepal. As the appointed external auditor, our team was tasked with evaluating the organization's information systems and security practices to identify potential vulnerabilities and provide recommendations for improvement.

The audit was conducted in accordance with relevant international standards and local regulations, employing a comprehensive methodology to assess Zenith Solutions' security posture. Our approach included document review, interviews with key personnel, technical assessments, and analysis of security logs and data which finally was followed by reporting of vulnerabilities found.

Organizational Structure for the Information Security Team at Zenith Solutions

The first response to tackling the challenges faced by Zenith Solutions is a robust and well-structured Information Security team. The following organization structure is designed to address these challenges which ensure the security measures are in proper place to protect the company's critical assets and data. This structure aligns with industry best practices and regulatory requirements.

Figure 1: Chart Demonstrating Information Security Team.

1. Chief Information Security Officer (CISO)

Reports to: CEO or Board of Directors

Responsibilities: Develop and implement company-wide information security strategy, oversee all aspects of the organization's information security program, collaborate with executive

leadership on security initiatives and risk management, ensure compliance with relevant laws and regulations, particularly those applicable to software development firms in Nepal.

2. SOC (Security Operations Center)

Manager Reports to: CISO

Responsibilities: Oversee daily SOC operations, manage, and coordinate the SOC team, develop and implement security monitoring strategies, ensure timely detection and response to security incidents, provide regular reports on security status to the CISO.

3. Security Analysts

Reports to: SOC Manager

Responsibilities: Monitor security events and alerts, analyze potential security threats, conduct initial investigations of security incidents, maintain security monitoring tools and systems, prepare detailed reports on security findings and incidents.

4. Incident Responders

Reports to: SOC Manager

Responsibilities: Lead the response to security incidents, conduct in-depth investigations of confirmed security breaches, develop, and maintain incident response plans, coordinate with other teams during incident handling, provide post-incident reports and recommendations.

5. Threat Hunter

Reports to: SOC Manager

Responsibilities: Proactively search for hidden threats within the network, develop and implement threat hunting strategies, analyze complex data sets to identify potential security risks, collaborate with other security teams to improve threat detection capabilities.

6. SIEM Manager

Reports to: SOC Manager

Responsibilities: Manage and optimize the Security Information and Event Management (SIEM) system, develop and maintain SIEM use cases and correlation rules, ensure proper log collection and retention, provide SIEM-related training to other team members.

7. Security Architect and Engineering Team Lead

Reports to: CISO

Responsibilities: Design and oversee implementation of security architecture, lead security engineering efforts across the organization, evaluate and recommend security technologies and solutions, collaborate with development teams to ensure secure software design, align security architecture with Zenith Solutions' software development processes.

8. Security Engineers

Reports to: Security Architect and Engineering Team Lead

Responsibilities: Implement and maintain security systems and infrastructure, conduct security assessments of new and existing systems, develop and enforce security standards and best practices, collaborate with development teams to integrate security measures into software products, assist in incident response and forensic analysis when needed.

9. Risk and Compliance Team Lead

Reports to: CISO

Responsibilities: Develop and maintain the organization's risk management framework, ensure compliance with relevant laws and regulations (especially those applicable to software development firms in Nepal), conduct regular risk assessments and audits.

10. Risk Management Officer

Reports to: Risk and Compliance Team Lead

Responsibilities: Identify and assess potential risks to the organization's information assets, develop and implement risk mitigation strategies, monitor and report on the effectiveness of risk management activities, collaborate with other teams to address identified risks.

11. Security Awareness and Training Coordinator

Reports to: Risk and Compliance Team Lead

Responsibilities: Develop and deliver security awareness training programs for all employees, create and maintain security policies and procedures, conduct regular security awareness campaigns, measure and report on the effectiveness of security awareness initiatives.

12. Data Privacy Officer

Reports to: Risk and Compliance Team Lead

Responsibilities: Ensure compliance with data protection laws and regulations, develop and implement data privacy policies and procedures, conduct privacy impact assessments, handle

data subject requests and complaints, provide guidance on privacy-related matters to other departments.

13. DevSecOps Specialist

Reports to: CISO

Responsibilities: Integrate security practices into the software development lifecycle, develop and implement secure coding standards, collaborate with development and operations teams to automate security processes, conduct security assessments of cloud environments and configurations.

14. Application Security Specialists

Reports to: DevSecOps Specialist

Responsibilities: Perform security code reviews, conduct application security testing, work with developers to remediate identified vulnerabilities, develop and maintain secure coding guidelines, provide security guidance during the software development process.

15. Cloud Security Specialist

Reports to: DevSecOps Specialist

Responsibilities: Assess and secure cloud infrastructure and services, develop and implement cloud security policies and procedures, monitor cloud environments for security threats, ensure compliance with relevant cloud security standards, collaborate with development teams to implement security best practices in cloud deployments.

16. CyberOps Engineer

Reports to: DevSecOps Specialist

Responsibilities: Automate security processes and controls, develop and maintain security-related scripts and tools, integrate security tools into the CI/CD pipeline, collaborate with development and operations teams to implement security measures throughout the software lifecycle, monitor and respond to security events in the development and production environments.

17. Penetration Testing Team Lead

Reports to: CISO

Responsibilities: Plan and oversee penetration testing activities, develop and maintain penetration testing methodologies, analyze test results and provide actionable recommendations, collaborate with other teams to address identified vulnerabilities, ensure compliance with relevant laws and regulations during testing activities.

18. Red Team

Reports to: Penetration Testing Team Lead

Responsibilities: Conduct external network and web application penetration tests, simulate real-world attack scenarios, identify and exploit vulnerabilities in external-facing systems, document findings and provide detailed reports, recommend security improvements based on test results.

Relevant Laws and regulation

As the CISO of Zenith Solutions, it is crucial to conduct an external audit of our Information system to tackle the IT security challenges the company has been facing lately. This audit will help evaluate security posture and identify vulnerabilities. To justify this audit, we must consider both international and national laws and regulations that govern data protection and information security.

Relevant National laws and regulations

1. **Electronic Transaction Act, 2063(2008) - Nepal**

   This act provides the legal framework for electronic transaction and digital signature in nepal. It also includes provisions for data protection and cybersecurity. (*Highlights of Electronic Transactions Act, 2006 (2063)*, 2022)v

Justification: As a software development firm, Zenith Solutions likely engages in numerous electronic transactions. Compliance with this act is essential to ensure the legality and security of these transactions.

2. **Privacy Act, 2075 (2018) - Nepal**

   This act aims to protect the privacy rights of individuals and regulates the collection, use, and disclosure of personal information by organizations. (Pa7175Z, 2022)

Justification: If Zenith Solutions handles personal data of clients or employees, compliance with this act is mandatory. An external audit will help ensure that our data handling practices meet the requirements of this law.

Relevant International laws and regulations

1. General Data Protection Regulation (GDPR) - European Union

Although not a Nepali law, GDPR has global implications for companies handling data of EU citizens. (*General Data Protection Regulation (GDPR) – Final Text Neatly Arranged*, 2024)

Justification: If Zenith Solutions has clients or users from the EU, or processes data of EU citizens, compliance with GDPR is crucial. An external audit can help identify any gaps in GDPR compliance.

2. Payment Card Industry Data Security Standard (PCI DSS)

Global Standard Although not a specific law, PCI DSS is a global security standard that must be followed by all organizations that handle credit card information. (PCI Security Standards Council, 2018)

Justification: Given that Zenith Solutions uses various payment systems in their software, compliance with PCI DSS is crucial. This standard helps protect cardholder data and reduce the risk of data breaches.

3. ISO/IEC 27034-1:2011 - Application Security

While not a law, ISO/IEC 27034-1 provides a comprehensive framework for integrating security into the entire application lifecycle. It covers secure design, development, testing, deployment, and maintenance of applications.

Justification: As a software development firm, Zenith Solutions is inherently involved in creating and managing applications. Adhering to ISO/IEC 27034-1 ensures that security is embedded into

the software development process, reducing the risk of vulnerabilities and enhancing the overall security of the company's products.

4. **NIST Special Publication 800-53 - Security and Privacy Controls for Information Systems and Organizations**

Although primarily applicable to U.S. federal agencies, NIST SP 800-53 is widely recognized and adopted as a comprehensive catalog of security and privacy controls for information systems and organizations. (NIST, 2021)

Justification: Even though Zenith Solutions is based in Nepal, aligning with NIST SP 800-53 demonstrates a commitment to robust security practices and can be beneficial when dealing with international clients or partners who may require adherence to such standards

Audit Methodology: ISO 27001

As Zenith Solutions have grown, so have the complexities of the information system and the associated security risks. Given the sensitive nature of client data and proprietary software code zenith solution handles having a great security is must.

To address the challenges faced and conduct an external audit of Zenith Solution's information systems, the ISO/IEC 270001 Information Security Management System (ISMS) is our primary framework, except that the laws and regulations mentioned earlier will be also considered during the audit.

ISO 27001 is an widely recognized standard which provides a systematic approach to manage sensitive company information. It encompasses people, processes, and IT systems by applying a risk management process.

We have selected ISO 27001 for several key reasons:

1. **Holistic Approach**: ISO 27001 covers technical, organizational, and human aspects of information security, providing a comprehensive assessment framework.
2. **Global Credibility:** As the standard is internationally recognized it will open the company to international business opportunities.
3. **Risk Management Focus:** The standard's emphasis on risk assessment and mitigation is crucial for a software development firm like Zenith Solutions.

Overview of Audit Methodology based on ISO 2700:

Figure2: Audit Methodology

1. Initial Assessment and scoping

The audit will start by defining the audit scope, identifying key stakeholders, and understanding Zenith Solutions' business context. This phase includes meetings with management to set expectations and gather initial information.

2. Risk Assessment

A thorough risk assessment is conducted to identify potential threats to the company's information assets which involved analyzing potential impact of various risk specific to the software development industry.

3. Gap Analysis Against ISO27001 Controls

All the current company's practices will be compared against the 114 controls outlined in ISO 27001 Annex A. The idea behind this is to help us identify where the company security measures fall short on the standard requirements.

4. Review of Existing Policies and Procedures

The company's current information security policies and procedures will be reviewed and compared to verify whether it aligns with ISO 27001 and industry best practices.

5. Technical Assessment

This involves all the technical evaluations, including vulnerability scans and penetration tests, to assess the security of the company's IT infrastructure. This phase may also include review of access controls, network security and data protection measured depending upon the necessity.

6. Interviews and Observations

Key personnel across different departments will be interviewed to understand how security policies are implemented in practice. Also, the company's day-to-day operations will also be observed to verify the adherence to security measures.

7. Evidence Collection and Analysis

We will also gather and analyze differnt evidence to support our findings, this may include system logs, security incident reports and other documents that are relevant.

8. Reporting and recommendations

The findings from the audit will be compiled into a comprehensive report, highlighting areas of compliance and identifying gaps followed by providing actionable recommendations for improvement. The report will include an executive summary for management and detailed technical findings for the IT staff.

System Audit is a big process and the existing frameworks like ISO 27001 are just the guidelines and not a complete package for everything. Audits face so many problems while we are following only guidelines only so there should be a proper plan in case of any problems faced during the Aduit. The below given is the audit flowchart for the Zenith company which is strictly followed by the Information team while conducting the audit.

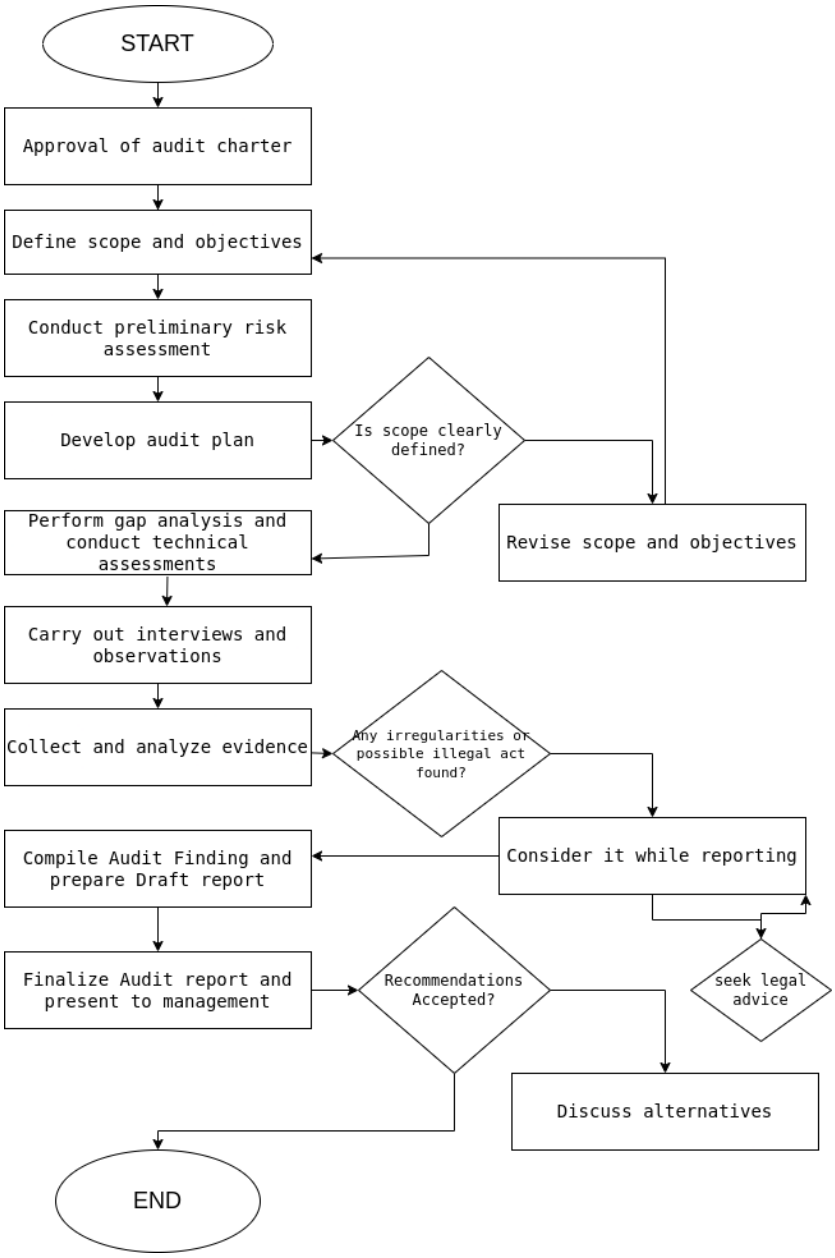

Figure3: Audit Flowchart

Step-By Step Audit Techniques

As the methodology for the audit is ISO 27001 so follows our audit steps. We have incorporated the guidelines given by ISO 27001 and followed a step-by-step process for the system audit of the company. After the pre-planning phase included scope definition all the below step were done one by one.

Figure4: Audit steps

1. Planning and Scoping

The primary objectives of this phase is to establish clear understanding of audit purposes, boundaries and to develop well-structured plan for execution. The **scope** of the audit will be explicitly outlined, encompassing the specific systems, processes, and data that will be subject to scrutiny. The audit will specifically target areas crucial to software development, such as:

- **Source Code Repositories**: Security of code repositories like GitHub or Bitbucket, including access controls, code review processes, and vulnerability scanning of code.

- **CI/CD Pipelines**: Security of the Continuous Integration/Continuous Deployment (CI/CD) pipelines, including secure coding practices, vulnerability scanning during builds, and secure deployment processes.
- **Cloud Infrastructure**: Security of cloud services used for development, testing, or deployment, including proper configuration of cloud resources, access controls, and data encryption.
- **Network security**: The and security of network devicesl such as firewalls, routers, switches, and wireless access points will be evaluated
- **Web application**: The security of external-facing web applications and APIs will be thoroughly examined.

Audit plan

A well-structured audit plan will serve as a roadmap for the entire process so below is what our audit plan for the company looks like.

Figure5: Audit Plan

Sampling Methodology

As the company's information system is vast it's often not very practical to examine everything. So, a combination of **stratified sampling and risk-based sampling** will be used. Stratified sampling will ensure that different types of systems and processes, including network devices and web applications, are adequately represented in the audit sample. Risk-based sampling will prioritize areas of higher risk, such as systems handling sensitive data or critical business functions.

Evidence Collection and Handling

The audit process relies heavily on the collection and analysis of evidence to support findings and recommendations. The types of evidence to be gathered will be explicitly defined, encompassing:

- **System Logs**: Security logs, application logs, and audit trails from critical systems and applications.
- **Configuration Files**: Network device configurations, firewall rules, access control lists, and cloud service configurations.
- **Interview Notes**: Documentation of discussions with key personnel, including developers, system administrators, and management.
- **Screenshots**: Visual evidence of system configurations, vulnerabilities, or security incidents.
- **Vulnerability Scan Reports**: Results from automated security scanning tools used to assess code repositories, web applications, and cloud infrastructure.
- **Code Snippets**: Examples of secure and insecure coding practices identified during code reviews.
- **Third-Party Documentation**: Security assessments or certifications provided by third-party vendors or service providers.
- **Network Diagrams and Documentation**: Network topology diagrams, firewall rule sets, and other relevant network documentation.
- **Web Application Security Configurations**: Security settings for web servers, application firewalls, and other web application security controls.

- **Network Security Logs**: Logs from firewalls, intrusion detection/prevention systems, and other network security devices.

2. Risk Assessment and Gap Analysis

The risk assessment at Zenith Solutions identified and evaluated potential threats to the company's information assets, considering both the likelihood of occurrence and the potential impact on the business. The following table summarizes some of the key risks identified, along with their potential impact and likelihood ratings:

Risk Category	Specific Risk	Potential Impact	Likelihood	Overall Risk Rating
External Threats	Data breach due to cyberattack	High	Medium	High
	Intellectual property theft	High	Medium	High
	Disruption of operations due to ransomware attack	High	Medium	High
Internal Threats	Accidental data leaks by employees	Medium	Medium	Medium
	Unauthorized access by employees	Medium:	Low	Low
	Malicious insider activity	High	Low	Medium
Technology Risks	Vulnerabilities in software or cloud infrastructure	High	High	High
	Outdated or unsupported technologies	Medium	Medium	Medium
	Supply chain attacks	High	Low	Medium
Business Process Risks	Inadequate change management processes	Medium	Medium	Medium
	Weak incident response capabilities	High	Medium	High

Figure6: Risk assessment of company

The gap analysis of Assets of the company against ISO 27001 controls showed the potential gaps in the company.

Area	ISO 27001 Control	Potential Gap	Risk
Source Code Management	A.14.2.5 - Secure development environment	Lack of code review process or inadequate enforcement	Introduction of vulnerabilities or insecure coding practices into production code
CI/CD Pipeline	A.14.2.1 - Security in development and support processes	Absence of automated security testing within the CI/CD pipeline	Deployment of vulnerable code or configurations into production environments
Cloud Infrastructure	A.13.1.1 - Network controls	Overly permissive access to cloud resources or inadequate network segmentation	Unauthorized access to sensitive data or lateral movement within the cloud environment
Network Security	A.13.1.3 - Secure configuration of network devices	Outdated firmware or misconfigured firewall rules	Exploitation of known vulnerabilities or unauthorized network access
Web Application Security	A.12.6.1 - Management of technical vulnerabilities	Lack of regular web application penetration testing or inadequate input validation	Exploitation of web application vulnerabilities like SQL injection or XSS, leading to data breaches or system compromise
Access Control	A.9	Excessive privileges granted to user accounts	Unauthorized access to sensitive data or systems
Asset Management	A.8	Lack of a comprehensive inventory of information assets	Difficulty in identifying and prioritizing critical assets, potential for asset loss or theft
Human Resource Security	A.7	Inconsistent background checks for new hires	Potential for hiring individuals with malicious intent or a history of security breaches
Physical and Environmental Security	A.11	Inadequate physical security measures at premises	Unauthorized physical access to critical systems or data
Information Security Incident Management	A.16	Lack of a formal incident response plan or infrequent testing	Increased impact of security incidents due to delayed or ineffective response
Supplier Relationships	A.15	Lack of clear security requirements in contracts with third-party vendors	Security breaches or data leaks through third-party vendors

Figure7: Gap analysis

3. Vulnerability analysis and Technical Assessment

The third phase, **Technical Assessment and Vulnerability Analysis**, dives deep into Zenith Solutions' technological infrastructure and software development practices to actively identify and exploit potential weaknesses.

- **Network Vulnerability Scanning**: The audit employed **Nessus Professional** to conduct comprehensive scans of Zenith Solutions' network infrastructure.
- **Cloud Infrastructure Assessment**: The security of Zenith Solutions' cloud environments was evaluated using **AWS Inspector** for Amazon Web Services and **Azure Security Center** for Microsoft Azure resources.
- **Web Application Security Analysis**: Web application security was assessed using a combination of automated and manual testing techniques. **OWASP ZAP (Zed Attack Proxy)** was deployed for dynamic web application scanning.

- **Code Review**: A comprehensive code review was performed on Zenith Solutions' critical applications. The audit team utilized static code analysis tools like **SonarQube** and manual review techniques to examine the source code.
- **Log Analysis**: The audit conducted comprehensive log analysis using advanced tools like **Wazuh**. This process involved examining system logs, network traffic, and application data to identify potential security threats, unusual patterns, and compliance issues.
- **Social Engineering Testing**: To evaluate the human element of Zenith Solutions' security posture, controlled social engineering tests were conducted.

The vulnerability Analysis revealed the potential vulnerability existing in the system which coudl very easily be exploited by the threat actor. So acting like a real threat actor a penetration testing was then conducted on the company.

Source Code Management

- **Exploiting Lack of Code Reviews**: The penetration testers manually reviewed code commits that bypassed the code review process, focusing on recent changes and bug fixes
- **Exploiting Outdated Security Scanner**: The penetration testers leveraged known vulnerabilities in open-source libraries that were not detected by the outdated security scanning tool.

CI/CD Pipeline

- **Exploiting Lack of SAST and SCA**: The penetration testers introduced vulnerable code snippets and outdated dependencies into the codebase. The CI/CD pipeline failed to detect these issues, allowing them to propagate to the staging environment.

- **Bypassing Security Gates**: The penetration testers triggered a critical vulnerability alert during a build process. However, they bypassed the security gate by manually overriding the alert, showing the potential for unauthorized deployment of vulnerable code.

Cloud Infrastructure

- **Exploiting Overly Permissive IAM Policies**: The penetration testers utilized a compromised low-privilege user account and exploited an overly permissive IAM policy to escalate their privileges and gain access to sensitive data in an S3 bucket.
- **Exploiting Misconfigured S3 Buckets**: The penetration testers identified S3 buckets with public access and successfully downloaded sensitive data, demonstrating the potential for unauthorized data exposure.

Network Security

- **Exploiting Outdated Firmware**: The penetration testers targeted a network device with known vulnerabilities in its outdated firmware. They successfully exploited a remote code execution vulnerability, gaining control of the device and potentially pivoting to other parts of the network.
- **Bypassing Firewall Rules**: The penetration testers crafted network traffic to bypass poorly configured firewall rules, demonstrating the potential for unauthorized access to internal systems.

Web Application Security

- **Exploiting SQL Injection**: The penetration testers successfully exploited the SQL injection vulnerability in the customer login form, extracting sensitive customer data from the database.

- **Exploiting XSS**: The penetration testers injected malicious JavaScript code into the user profile page, demonstrating the potential for stealing user sessions or executing arbitrary code in the context of other users' browsers.
- **Bypassing WAF**: The penetration testers crafted requests to bypass the outdated web application firewall (WAF), successfully delivering malicious payloads to the web application.

The penetration testing revealed a lot of weaknesses in the company and this evidence were collected based on the sample methodology we defined.

4. Interview and document review

The audit process also included an Interview and Document Review phase to gain a deeper understanding of Zenith Solutions' security policies, procedures, and employee awareness. The following activities were conducted:

Document Review: The audit team meticulously reviewed Zenith Solutions' key security documentation, including policies, procedures, incident response plans, and any relevant compliance documentation. The review aimed to assess the completeness, accuracy, and alignment of these documents with industry best practices and regulatory requirements.

Interviews: The audit team conducted interviews with key personnel across various departments, including IT, security, human resources, and management. The interviews focused on understanding the practical implementation of security policies, employee awareness of security risks, and the company's overall security culture.

5. Reporting and Follow-up

This final stage of the ISO 27001 audit process is the Reporting and Follow-up. This crucial step involves compiling a comprehensive audit report that summarizes all findings. The report is then presented to senior management, highlighting critical issues and recommended actions. Based on these findings, a corrective action plan is developed to address identified weakness found and implement suggested improvements. To ensure ongoing compliance and effectiveness of the implemented measures, follow-up audits are scheduled and conducted. This phase not only provides Zenith Solutions with a detailed overview of its current information security posture but also establishes a clear roadmap for continuous improvement and maintenance of ISO 27001 for the company.

Discovered Vulnerabilities

The ISO 27001 audit of company revealed many vulnerabilities in the different areas of the company. Wheather it was inadequate security awareness among the employees of improper access control in cloud all these will affect the company severely. The 4 vulnerabilities found in company revealed by audit are documented below:

Vulnerability #1: Outdated Patch Management Process

Introduction

The external audit of Zenith Solutions revealed an outdated and inefficient patch management process, posing significant risks to the company's security posture and operational efficiency.

Relevant Standard

ISO/IEC 27001:2013, control A.12.6.1, which requires timely management of technical vulnerabilities. (*ISO 27001 – Annex A.12: Operations Security*, 2020)

Description and Associated Risks

Zenith Solutions lacks a systematic approach to patch management. Key issues include:

I. Incomplete inventory of systems requiring updates
II. Delayed patch deployment
III. No clear prioritization for critical patches
IV. Some systems run unsupported software versions.

Risks include increased vulnerability to cyberattacks, potential data breaches, compliance violations, and operational disruptions.

Recommendations

I. Implement an automated patch management solution.

II. Develop a comprehensive system inventory.

Company Response

Zenith Solutions commits to implementing a robust patch management process. The IT department will propose a solution within 30 days, with full implementation expected within 90 days (about 3 months) from this report.

Vulnerability #2: Weak Cloud Security Configuration

Introduction

A major weakness in cloud security configuration, exposing the company to potential data breaches and unauthorized access. **Relevant Standard**

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), specifically domain Infrastructure & Virtualization Security (IVS-01 to IVS-13). (*CSA*, 2024)

Description and Associated Risks

Key issues in Zenith Solutions' cloud configuration include:

I. Overly permissive Identity and Access Management (IAM) policies

II. Misconfigured storage buckets with public access

III. Inadequate network segmentation in cloud environments

Risks include unauthorized data access, data leakage, potential compliance violations, and reputational damage from security incidents.

Recommendations

I. Implementing least privilege for all IAM policies.

II. Conduct a comprehensive review of storage bucket permissions.

III. Enhance network segmentation in cloud environments.

Company Response

The Cloud Security team will conduct an immediate review of current configurations. A remediation plan will be developed within 14 days (about 2 weeks), with full implementation of security enhancements expected within 60 days (about 2 months) from this report.

Vulnerability #3: Insufficient Employee Security Awareness

Introduction

The external audit revealed a significant lack of security awareness among Zenith Solutions' employees, increasing the risk of human-related security incidents.

Relevant Standard

NIST SP 800-50 "Building an Information Technology Security Awareness and Training Program" (Wilson & Hash, 2003)

Description and Associated Risks

Key issues identified include:

I. Lack of regular, comprehensive security awareness training

II. Employees are not properly aware of current cyber threats and different phising techniques.

III. Poor understanding of data handling and privacy policies

Risks include increased susceptibility to social engineering attacks, accidental data breaches, and non-compliance with data protection regulations.

Recommendations

I. Implement a structured, ongoing security awareness program.

II. Develop role-specific security training modules.

III. Establish a security champion program within departments.

Company Response

Zenith Solutions recognizes the critical need for improved employee security awareness. The HR and IT Security departments will collaborate to develop a comprehensive awareness program. Initial training materials will be ready within 45 days, with full program implementation expected within 90 days from this report.

Vulnerability #4: Inadequate Access Control Management

Introduction

The weak access control management will potentially allow unauthorized access to sensitive systems and data.

Relevant Standard

NIST SP 800-53 Rev. 5, Access Control (AC) family of controls (Peacock, 2024)

Description and Associated Risks

Key issues identified include:

I. Lack of a centralized identity and access management system
II. Excessive privileges granted to user accounts.
III. Inadequate monitoring of user activities and access patterns
IV. Inefficient process for revoking access rights for departing employees.

Risks include unauthorized data access, potential for insider threats, compliance violations, and difficulty in tracking and auditing user activities.

Recommendations

I. Implement a centralized Identity and Access Management (IAM) solution.
II. Enforce the principle of least privilege across all systems.
III. Establish a regular access rights review process.

Company Response

The company knows the critical nature of this vulnerability. The IT Security team will begin

implementing a new IAM solution within 30 days. Full implementation, including policy updates and staff training, is expected to be completed within 120 days from this report.

Appendix-I

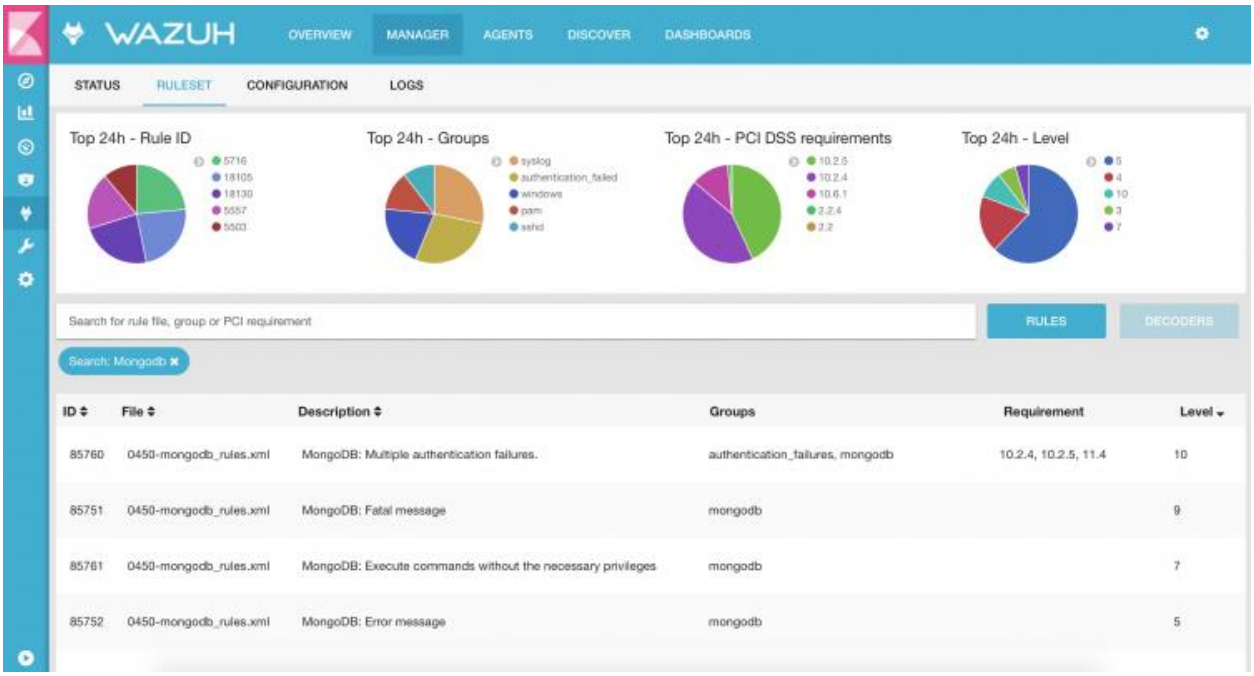

Figure8: Wazuh for analysis

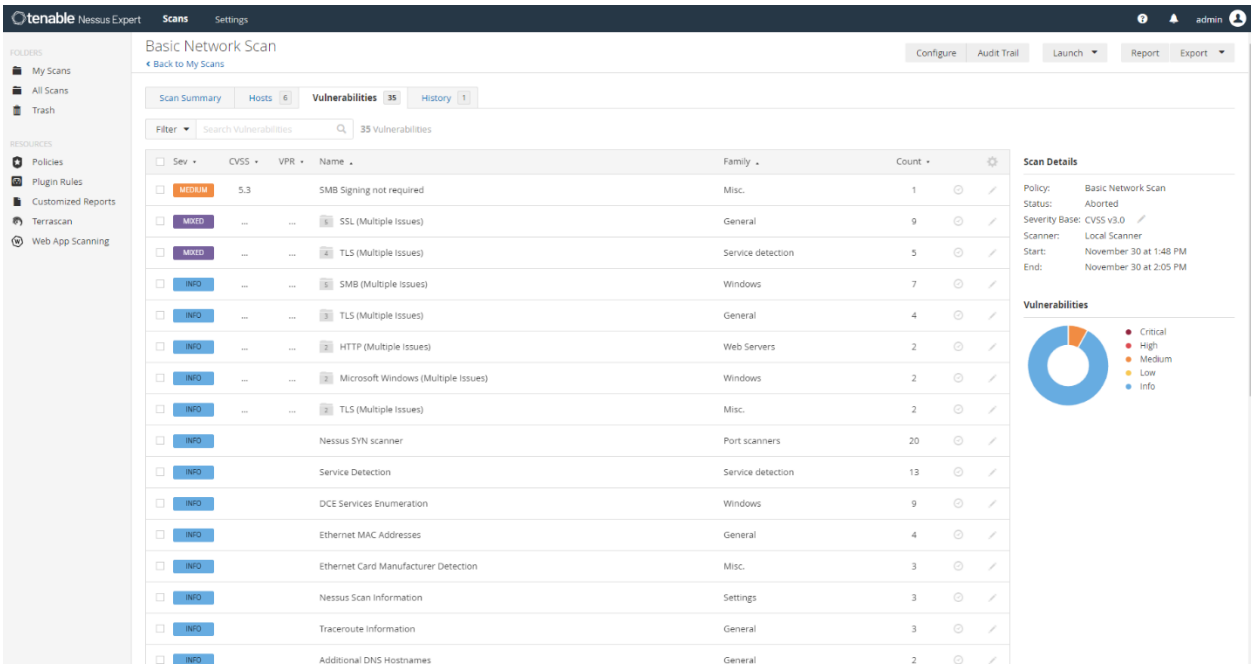

Figure9: Nessus Scanning Vulnerabilities

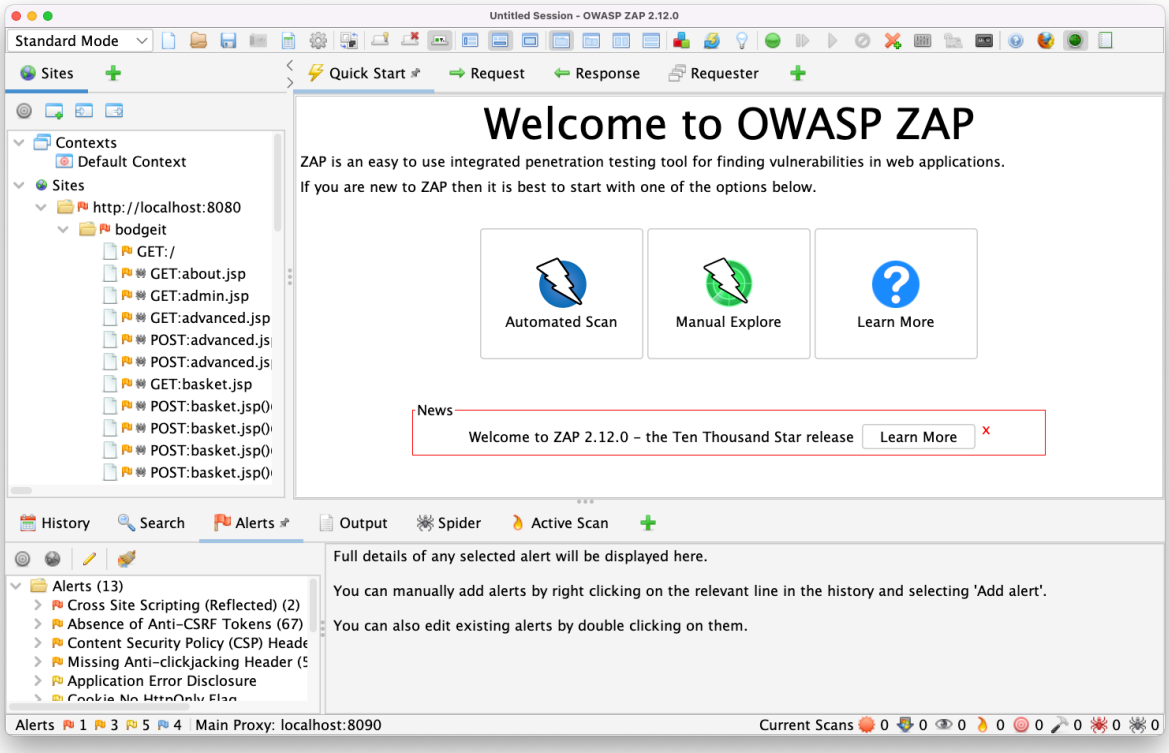

Figure10: OWASP ZAP for web analysis

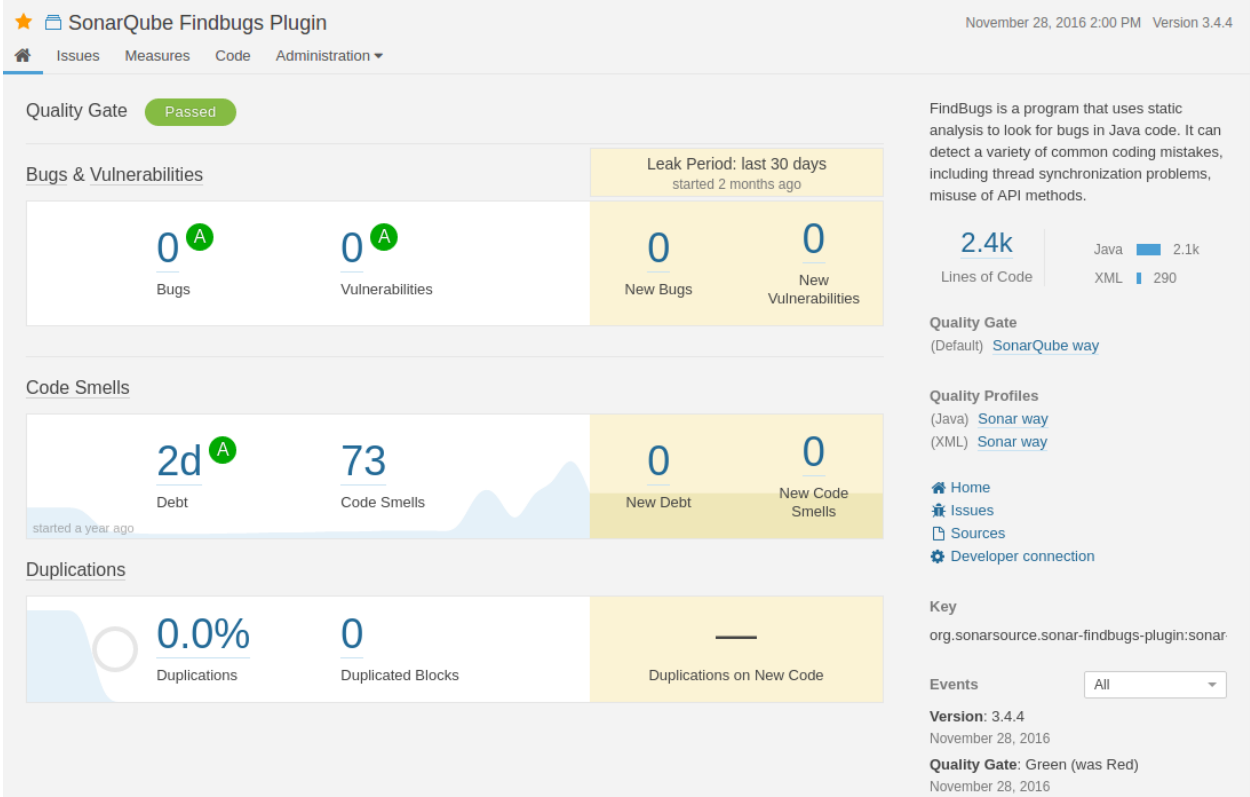

Figure11: SonarQube code analysis

Appendix-II

Avisha Co.

Audit Charter

INTRODUCTION

This external audit charter outlines the framework for conducting an independent assessment of Zenith Solutions' information systems and security practices. As a software development firm based in Nepal, Zenith Solutions recognizes the critical importance of maintaining robust information security measures. The purpose of this external audit is to evaluate the organization's current security posture, identify potential vulnerabilities, and provide recommendations for improvement.

SCOPE

- Network infrastructure and security controls
- Cloud configurations and code review
- Application development and deployment processes
- Data protection and privacy measures
- Access control and identity management
- Incident response and business continuity planning
- Compliance with relevant industry standards and regulations

OBJECTIVES

- Assess the overall effectiveness of Zenith Solutions' information security management system
- Identify potential vulnerabilities and security gaps in the company's IT infrastructure and processes
- Evaluate compliance with relevant industry standards, regulations, and best practices
- Provide actionable recommendations to enhance the organization's security posture and mitigate identified risks

AUDIT METHODOLOGY

The external audit will use ISO 27001 as the primary framework while also incorporating other relevant frameworks and guidelines.

TIMELINE AND MILESTONES

- Audit Planning and Preparation: 8/01/2024 - 8/15/2024
- On-site Audit Activities: 8/16/2024 - 11/25/2024
- Data Analysis and Report Drafting: 9/01/2024 - 11/30/2024
- Draft Report Submission: 12/01/2024
- Management Review Period: 12/01/2024 - 12/10/2024
- Final Report Presentation: 12/10/2024

References

- *Highlights of Electronic Transactions Act, 2006 (2063)*. (2022, August 28). Imperial Law Associates | Corporate Law Firm in Nepal. https://www.lawimperial.com/highlights-of-electronic-transactions-act-2006/#:~:text=The%20Electronic%20Transactions%20Act%202063,such%20records%20through%20illegal%20manner.
- Pa7175Z. (2022, January 6). *Individual Privacy Act, 2018 (2075) - Leading Law Firm in Nepal | Law Firm in Kathmandu | Pioneer Law Associates*. Leading Law Firm in Nepal | Law Firm in Kathmandu | Pioneer Law Associates. https://pioneerlaw.com/individual-privacy-act-2018-2075/
- *General Data Protection Regulation (GDPR) – Final text neatly arranged*. (2024, April 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/
- PCI Security Standards Council. (2018). *PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 3.2.1 For merchants and other entities involved in payment card processing*. https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
- NIST. (2021). Security and Privacy Controls for Federal Information Systems and Organizations. *NIST*. https://doi.org/10.6028/nist.sp.800-53r4
- (2024). Iso.org. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27034:-1:ed-1:v1:en
- *CSA*. (2024). CSA. https://cloudsecurityalliance.org/research/cloud-controls-matrix
- Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program*. https://doi.org/10.6028/nist.sp.800-50
- Peacock, J. (2024). *NIST SP 800-53 Control Families Explained*. Cybersaint.io. https://www.cybersaint.io/blog/nist-800-53-control-families#:~:text=The%20AC%20Control%20Family%20consists,and%20their%20level%20of%20access.

- *ISO 27001 – Annex A.12: Operations Security*. (2020). ISMS.online. https://www.isms.online/iso-27001/annex-a-12-operations-security/
- for, O. (2022). *ISO/IEC 27001:2022*. ISO. https://www.iso.org/standard/27001