

|  |  |
| --- | --- |
| [NCC Global Assignment] | |
| Candidate Name: | Thar Linn Htet |
| Candidate ID Number: | 202973 |
| Center Name: | KBT001 - KBTC College (School of IT) |
| Unit: | Network Security and Cryptography [NSC] |
| Qualification: | L5DC |
| Date: | 10/10/2025 |
| Total Word Counts: | 1982 |

Table of Contents

[1 Task 1 – Risk Assessment 2](#_Toc211036682)

[1.1 Five most important electronically held information and data assets for WHA 2](#_Toc211036683)

[1.2 Asset Risk Table 3](#_Toc211036684)

[2 Task – 2 Controlling the Risks – Explanation 5](#_Toc211036685)

[2.1 Recommendations to Reduce Identified Risks 5](#_Toc211036686)

[2.2 Vulnerability Identification and Remediation 6](#_Toc211036687)

[3 Task 3 – Securing the network 8](#_Toc211036688)

[4 Task 4 – Maintaining Security 11](#_Toc211036689)

[5 Task 5 – Reflective commentary 12](#_Toc211036690)

[References 14](#_Toc211036691)

# Task 1 – Risk Assessment

## Five most important electronically held information and data assets for WHA

Based on the WHA scenario, which is all about managing affordable housing and handling sensitive tenant info, we’re focusing on figuring out the most important digital assets.

1. **Tenants’ Personal Identification Information (PII) and Related Data:** This includes things like names, addresses, and other identifying info about tenants. PII is the most sensitive stuff WHA has. If it gets leaked, WHA would be breaking rules like GDPR, which could seriously hurt its reputation and cost a ton in fines.
2. **Payment and Financial Records:** These records include details regarding rent payments and other financial transactions. Losing these records could cause actual money loss for WHA, allow fraud, and make it hard to track income and expenses.
3. **Internal Database and File Servers:** These servers, located at the Manchester office, contain the web, file, and database systems that support WHA’s operations. If the internal servers are unavailable, all critical services go down immediately, including access to stored data, payment systems, and the ability for employees to work.
4. **Shared Cloud Storage Credentials ('**[**whaadmin@wha.co.uk**](mailto:whaadmin@wha.co.uk)**' and 's3c4ur3'):** These documents, often exchanged via email and WhatsApp, constitute the contractual and legal proof of WHA’s operations. Ensuring their confidentiality and integrity is mandatory, as unauthorized alteration or disclosure could lead to substantial legal risks and financial liability.
5. **Digital Lease Agreements and Legal Correspondence:** This includes legal documents exchanged with solicitors, lease agreements, and internal legal correspondence.These documents are confidential and legal proof of WHA's business relationships and property management duties. The leaks could lead to significant legal problems, financial matters.

## Asset Risk Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | CIA? | Likelihood | Impact | Risk |
| Tenants' PII & Financial Records | **External Data Breach/Hacking** (targeting known vulnerabilities in servers) | C, I | Medium | High | High |
| hared Cloud Storage Credentials | **Credential Theft/Phishing** (exploiting single shared password 's3c4ur3') | C, I, A | High | High | **Very High** |
| Central Database Server | **Hardware Failure** (System outage impacting availability) | A | Low | Medium | Low |
| Digital Lease Agreements & Legal Correspondence | **Loss of device/Interception** (data stored/exchanged via unmanaged personal smartphones/WhatsApp) | C | High | Medium | High |
| WHA Tenant Website Backend | **Denial of Service (DoS)** (preventing tenants from submitting requests/paying rent) | A | Medium | Medium | Medium |

# Task – 2 Controlling the Risks – Explanation

## Recommendations to Reduce Identified Risks

In task 1 (b), the potential threats and their highest risks are identified. In the following, the recommendations of countermeasures are provided for WHA to control and reduce them.

1.Shared Cloud Storage Credentials

The biggest threat is the use of a weak shared password. This password can lead to data loss when it gets leaked. To prevent that, Multi-Factor Authentication (MFA) should be implemented. MFA requires users to verify their identity through two or more factors, such as a password and a pass code (Journalist, 2025). The IAM system also allows employees to have an individual account instead of using a shared admin login (Gontovnikas, 2021).

2. Tenants’ Personal and Financial Information

Tenant data is one of WHA’s most sensitive assets. It is vulnerable to external attacks, especially through hacking. Encryption ensures that even if hackers steal data, it remains unreadable without decryption keys (Anonymus, -). Applying Role-Based Access Control (RBAC) to restrict access based on an employee’s role also covers the threats. For example, only finance staff can view payment data (Lindemulder, -).

3. Central Database Server

Outdated server software creates opportunities for attackers to exploit known vulnerabilities. A strong patch update ensures that all systems are updated and can reduce vulnerabilities before attackers can be exploited. Installing an Intrusion Prevention System (IPS) also detects and blocks suspicious activity in real time, acting as a frontline defense against exploitation attempts (Anonymus, -).

Digital Lease Agreements and Legal Correspondence

Legal documents are currently exchanged through personal messaging apps like WhatsApp. This is insecure and increases the risk of interception or data loss. A Mobile Device Management (MDM) policy can secure all employee devices, allow remote data wiping and enforce device encryption. Making sure all staff use a secure, organization-approved communication platform also prevents data loss (Team, 2025).

5. WHA Tenant Website Backend (Risk: High)

The new beta website handles tenant data and financial transactions. It is highly vulnerable to web-based attacks like SQL injection or cross-site scripting. Implement a Web Application Firewall (WAF) to filter malicious requests. It protects both the application and the database (Fortinet, -). Applying strict input validation in the website’s backend code also prevents attackers from inserting harmful scripts or commands (Anonymus, -).

## Vulnerability Identification and Remediation

WHA’s current network setup and software configurations have several weaknesses that can expose the organization to cyber threats. Understanding these vulnerabilities is vital to protect the system, sensitive tenant data, and maintain operational reliability.

**Known Software Vulnerabilities**

The internal servers at WHA, including web, file, and database servers, host several outdated or misconfigured software components.

1. The first major vulnerability is the **Apache Log4j 2 version 2.15**. This version is linked to the widely known **Log4Shell** exploit (CVE-2021-44228). The issue allows attackers to run remote code on the server. Even though version 2.15 attempted to fix the flaw, further research showed it still allowed (DoS) attacks under certain conditions. To fix this, WHA should update Log4j to version 2.17.1 or later. If an upgrade cannot be done immediately, disabling message lookups in configuration files can help reduce the risk.
2. The second vulnerability is the **Oracle WebLogic Server version 12.2.1.4.0**, which encounters deserialization flaws that can lead to Remote Code Execution (RCE). Attackers can exploit the **T3 protocol** to unauthorized access to sensitive files and databases. This issue has been documented in Oracle’s CVE advisories and remains a high-severity concern (Oracle, -). WHA should apply Oracle’s latest Critical Patch Updates (CPUs) or upgrade to a supported version. The T3 protocol should also be firewalled so that only trusted internal systems can access it.
3. A third vulnerability appears in **CoreFTP Server to build 725**. Older FTPs are known for overflowing weaknesses. Attackers can send crafted data to overload memory, which lets them inject malicious code or access private files. To prevent this, WHA should move from outdated FTP systems to **SFTP or FTPS**. If the current server must stay active, it should be updated to the most recent secure release.

**Network Vulnerabilities – Cloud Storage Service**

1. One problem is the **use of shared credentials** like “[whaadmin@wha.co.uk](mailto:whaadmin@wha.co.uk)” with a weak password. This makes it impossible to track user actions and easy for attackers to guess or leak the password. The solution is to create **individual user accounts** with strong passwords and clear access privileges.
2. Another vulnerability is the **absence of Multi-Factor Authentication (MFA)**. Without MFA, a single stolen password could give full access to cloud backups. Enabling MFA ensures can cover the password validation.

**Network Vulnerabilities – Tenant Website**

1. The beta tenant website’s weakness is **insecure communication** because it currently runs on **HTTP** instead of HTTPS. Any personal or financial data sent through HTTP can be intercepted during transmission. The best fix is to install an SSL/TLS certificate, switching to HTTPS before launching (Cloudflare, -).
2. **Injection attacks** such as **SQL Injection** or **Cross-Site Scripting (XSS)** can input validation allowing attackers to send malicious commands or scripts (PortSwigger, -). This led to unauthorized database access or stolen user sessions. WHA’s developers should use **clean queries**, sanitize all input, and encode output before displaying it on the page to block these types of exploits (Maury, 2025).

# Task 3 – Securing the network

Securing WHA’s network infrastructure requires a mix of technical solutions and structured access control. The main tools that can be used for WHA’s defenses include Virtual Private Networks (VPNs), Firewalls with a Demilitarized Zone (DMZ), and Intrusion Detection Systems (IDSs).

**a) Application of Virtual Private Network (VPN) Technology**

A Virtual Private Network (VPN) is essential for WHA because many employees access the internal network remotely. VPNs create an encrypted tunnel over public or untrusted networks, ensuring that all transmitted data remains unreadable to outsiders (Paloalto, -). This encryption protects against eavesdropping and Man-in-the-Middle attacks even when employees connect via public Wi-Fi at cafes or shared facilities. It also authenticates users, ensuring that only authorized employees can reach the Manchester office network (Team, 2025).

The most suitable type of VPN for WHA is a **Remote-Access VPN**, because it allows individual users to securely connect to the company’s internal systems from any location (Paloalto, -). This setup ensures that field workers and home-based employees can safely reach file and database servers without risking data interception.

**b) Use of Firewalls and a Demilitarized Zone (DMZ)**

Firewalls are the backbone of WHA’s network security. They filter traffic based on rules and policies. They should be configured to separate trusted and untrusted network segments. WHA must establish a **Demilitarized Zone (DMZ)** to strengthen the system, which isolates public-facing services—such as the tenant website from the organization’s internal network (Fortinet, 2025).

The DMZ serves as a protective buffer. The **perimeter firewall** should be positioned between the internet and the DMZ, that blocks malicious traffic before it reaches public servers. The tenant web server should be hosted within the DMZ so that even if it is breached, attackers cannot directly access sensitive internal data. A **second internal firewall** should separate the DMZ from the internal network, allowing only essential data to pass through. This dual-firewall approach provides layered protection against intrusions and ensures tenant and financial data remain secure even in case of an external attack.

A computer network diagram with icons

AI-generated content may be incorrect.

Figure WHA's Network Infrastructure

**c) Importance and Types of Intrusion Detection Systems (IDSs)**

Intrusion Detection Systems (IDSs) play an important role in identifying suspicious activities that may bypass the firewall. Unlike firewalls, which block traffic, IDSs monitor and alert administrators when they detect unusual or malicious patterns. This helps WHA maintain continuous awareness of its network health and respond quickly to potential breaches.

A **Network-based IDS (NIDS)** should be deployed near the firewalls and DMZ to monitor inbound and outbound traffic (Fortinet, -). It would help detect external attacks, such as attempts to exploit Log4j or WebLogic vulnerabilities, before they reach critical systems. Meanwhile, a **Host-based IDS (HIDS)** should be installed on internal servers like the database and file servers to monitor local activity, detect unauthorized file modifications, and flag privilege escalation attempts. Together, NIDS and HIDS form a layered defense mechanism, ensuring both external and internal threats are promptly identified and addressed (SysDig, -).

# Task 4 – Maintaining Security

To maintain security and uphold compliance, WHA must address its ongoing regulatory weaknesses, especially the use of unauthorized communication channels for handling sensitive tenant data.

**GDPR Breach via WhatsApp Messenger:**

The use of WhatsApp Messenger on personal devices to exchange information, legal correspondence, and personally identifiable information (PII) is a violation of the General Data Protection Regulation (GDPR) (Anonymus, -). GDPR requires organizations to ensure appropriate technical and organizational measures for data protection. By using a consumer-grade messaging app, WHA loses control over how data is stored, shared, or deleted.

**Role of Senior Management in Fostering Security Culture:**

Senior management plays a critical role in ensuring security compliance and establishing a culture of accountability. Leaders must demonstrate commitment to GDPR principles by introducing official communication policies, banning unauthorized apps, and deploying secure, compliant alternatives such as Microsoft Teams or encrypted email systems. Management should allocate resources for staff training, implement regular compliance audits, and enforce strict patch management schedules. By promoting consistent awareness and strong leadership, WHA can embed security into everyday operations and maintain a sustainable, compliant organization (CyBiz, 2023).

# Task 5 – Reflective commentary

Completing the WHA network security assignment gave me practical insight into how cybersecurity concepts apply in real-world situations. It helped me see the connection between theory and practice, especially when examining outdated systems like Apache Log4j and Oracle WebLogic.

**Learning and Problems Encountered:**

One of the biggest challenges was that the scenario didn’t include all the technical details I needed. That’s why I had to fill in the blanks using logical assumptions and extra research. Looking into CVEs and known vulnerabilities helped me connect what I learned in class to practical, real-life risks. It also gave me a better understanding of how confidentiality, integrity, and availability (the CIA triad) are affected when software isn’t configured or updated properly.

**Action Plan for Improvement:**

If I could restart the assignment, I would spend more time on the initial risk assessment to build a stronger foundation. Proper planning and clear mapping between risks and countermeasures would create a smoother, more coherent final report.

***[Word Count : 1982]***

# References

A Wondershare Company, E., 2024. *UML Class Diagram Examples.* [Online]   
Available at: https://www.edrawsoft.com/example-uml-class-diagram.html

A Wondershare Company, E., 2024. *UML Class Diagram Examples.* [Online]   
Available at: https://www.edrawsoft.com/example-uml-class-diagram.html

Anonymus, -. *cheatsheets/Input\_Validation\_Cheat\_Sheet.* [Online]   
Available at: https://cheatsheetseries.owasp.org  
[Accessed 4 October 2025].

Anonymus, -. *en/policies/data-protection-regulation/#:~:text=data%20protection%20rules-,What%20is%20the%20GDPR%3F,application%20on%2025%20May%202018..* [Online]   
Available at: https://www.consilium.europa.eu/  
[Accessed 7 October 2025].

Anonymus, -. *glossary/what-is-encryption/.* [Online]   
Available at: https://paramountassure.com/  
[Accessed 4 October 2025].

Anonymus, -. *topics/intrusion-prevention-system.* [Online]   
Available at: https://www.ibm.com/think/  
[Accessed 4 October 2025].

Cloudflare, -. */learning/ssl/how-does-ssl-work/.* [Online]   
Available at: https://www.cloudflare.com/  
[Accessed 5 October 2025].

CyBiz, 2023. *senior-managements-role-in-cybersecurity.* [Online]   
Available at: http://cybiz.au/  
[Accessed 8 October 2025].

Fortinet, 2025. *resources/cyberglossary/what-is-dmz.* [Online]   
Available at: https://www.fortinet.com/resources/  
[Accessed 6 October 2025].

Fortinet, -. *resources/cyberglossary/intrusion-detection-system.* [Online]   
Available at: https://www.fortinet.com/  
[Accessed 6 October 2025].

Fortinet, -. *resources/cyberglossary/waf-vs-firewall#:~:text=WAFs%20defend%20against%20application-layer,their%20focus%20on%20network%20traffic..* [Online]   
Available at: https://www.fortinet.com/  
[Accessed 4 October 2025].

Gontovnikas, M., 2021. *blog/what-is-iam/.* [Online]   
Available at: https://auth0.com/  
[Accessed 4 October 2025].

Journalist, E., 2025. *news/the-role-of-mfa-in-cybersecurity-strengthening-protection?ca.* [Online]   
Available at: https://vivatechnology.com/  
[Accessed 4 October 2025].

Lindemulder, G., -. *think/topics/rbac.* [Online]   
Available at: https://www.ibm.com/  
[Accessed 4 October 2025].

Maury, J., 2025. *endpoint/prevent-web-attacks-using-input-sanitization/.* [Online]   
Available at: https://www.esecurityplanet.com/  
[Accessed 5 October 2025].

Oracle, -. *security-alerts/alert-cve-2020-14750.html.* [Online]   
Available at: https://www.oracle.com/  
[Accessed 5 October 2025 ].

Paloalto, -. *cyberpedia/what-is-a-remote-access-vpn.* [Online]   
Available at: https://www.paloaltonetworks.com/  
[Accessed 6 October 2025].

Paloalto, -. *cyberpedia/what-is-a-vpn.* [Online]   
Available at: https://www.paloaltonetworks.com/  
[Accessed 5 October 2025].

PortSwigger, -. *web-security/cross-site-scripting.* [Online]   
Available at: https://portswigger.net/  
[Accessed 5 October 2025].

SysDig, -. *learn-cloud-native/what-is-hids.* [Online]   
Available at: https://www.sysdig.com/  
[Accessed 6 October 2025].

Team, S., 2025. *mobile-device-management-policy-key-strategies/.* [Online]   
Available at: https://symmetrium.io/  
[Accessed 4 October 2025].

Team, W. E., 2025. *academy/man-in-the-middle-attack.* [Online]   
Available at: https://www.wiz.io/  
[Accessed 6 October 2025].