



BSc (Hons) Ethical Hacking and Network Security

COBSCEHNS24.1P

Audit Report & Risk Treatment Plan

Assignment 01

Student Name: P. D. S. D. JAYATHILAKE

Coventry Index Number: 15386478

NIBM Index Number: COBSCEHNS24.1P-006

Consultant/Lecturer: K.H.C.R. Bandara

Faculty of Engineering, Environment and Computing

School of Computing, Electronics and Mathematics

Coventry University, London.

School of Computing

National Institute of Business Management

Colombo 07.

April 2025

TABLE OF CONTENT

LIST OF TABLES	3
LIST OF FIGURES.....	3
CYBERSECURITY AUDIT REPORT: Doha Bank It Systems Review	4
INTRODUCTION.....	4
AUDIT OBJECTIVES.....	5
AUDIT SCOPE.....	6
AUDIT METHODOLOGY.....	7
EXECUTIVE SUMMARY.....	8
AUDIT FINDINGS OBSERVATIONS AND RISK ASSESSMENT.....	9
RISK ASSESSMENT PLAN	19
RISK TREATMENT PLAN FOR AUDIT FINDINGS.....	21
AUDIT CONCLUSION	22
MANAGEMENT RESPONSE	23
APPENDICES	24
AUDITOR'S CERTIFICATION AND CONCLUSION.....	26
END OF THE AUDIT REPORT.....	26
REFERENCES.....	27

LIST OF TABLES

Table 1: Risk assessment plan for audit findings.	20
--	----

LIST OF FIGURES

Figure 1: Unpatched System Servers (Web Server-Ubuntu)	24
Figure 2: Inactive user accounts on the System	24
Figure 3: Missing security patches & antivirus updates on workstation computers	25
Figure 4: Nessus Vulnerability Scan Results on Servers	25

CYBERSECURITY AUDIT REPORT: Doha Bank It Systems Review

Date: March 30th, 2025.

Prepared by: Devmith Subashana Jayathilake (Internal IT Lead Auditor).

INTRODUCTION

This report explains the results of an internal cybersecurity audit of Our Doha Bank Head Office. Our Bank is a mid-sized bank offering retail and corporate banking services, including online banking, mobile banking and ATM services. Recently, the IT security team conducted a cybersecurity audit to assess compliance with industry standards such as ISO 27001 and PCI-DSS. The audit focused on network security, access controls, endpoint security, application security, incident response, third-party security and business continuity planning. Several security gaps and non-compliance issues were identified that could expose the bank to cyber threats, financial fraud, and reputational damage. The Board of Directors has requested a detailed audit report and a risk treatment plan to mitigate the identified security risks and ensure compliance with regulatory requirements. According to the request from the Board of Director's this document includes risk treatment plan to mitigate the identified security risks and ensured bank IT system complied with regulatory requirements.

AUDIT OBJECTIVES

The primary objectives of the internal audit:

- assess compliance with industry standards such as ISO 27001 and PCI-DSS.
- Focused on Identifying security risks that could impact on the bank's operations, bank's reputation, or financial stability under these areas such as network security, access controls, endpoint security, application security, incident response, third-party security and business continuity planning in the bank IT infrastructure.
- Focused on, The Board of Director's requested detailed audit report and a risk treatment plan to mitigate identified risks and improve the bank's cybersecurity posture with actionable and valuable recommendations.

AUDIT SCOPE

The audit focused on the bank's internal IT systems cybersecurity posture, including online banking, mobile banking, and ATM services, during the period from January 1st to March 30th in 2025. This audit covered the following areas of Our Bank's IT systems:

- Network security (Firewalls rules, System patching, Network segmentation)
- Access controls (Privileged access for users, MFA, User account management)
- Endpoint and workstation security (EDR, Antivirus, Device control)
- Web and application security (API security, input validation, Hardcoded credential management)
- Incident response and security monitoring (Documentation in IRP, SOC operations Monitoring, log retention times)
- Third-party vendor security (System access controls of Third-parties, Third-party companies security compliance)
- Business continuity and disaster recovery planning (DR testing, redundancy planning)

AUDIT METHODOLOGY

The audit was conducted using a combination of the following methods:

- **Interviews:** Discussions with the Staff members that interact with the IT and IT security processes, to understand processes and controls of their work.
- **Control Testing:** firewalking and testing of security controls, including access management, EDR and firewall rules & configurations.
- **Vulnerability Scanning:** Use of software like Nessus to identify unpatched systems and security vulnerabilities in the bank IT system.
- **Documentation Review:** Analysis of whether there are any missing policies, procedures, guidelines and logs, with the compliance in the documentation procedures.
- **Sampling:** Review and test randomly choose user accounts, workstations, and applications.
- **IT Security awareness campaign for Staff members:** to identify the vulnerable employees in the Staff And train them to become safe with cyber hygiene.

EXECUTIVE SUMMARY

The internal audit team identified critical nineteen cybersecurity gaps across multiple areas, including Network Security, Access Controls, Endpoint Security, Web Application Security, Security Monitoring & Incident Response, Third-Party Vendor Security and Business Continuity & Disaster Recovery plans. These vulnerabilities expose the Bank to significant risks, such as cyber threats, financial fraud, reputational damage and non-compliance with regulatory standards like PCI-DSS and ISO 27001. The bank needs to fix these issues immediately to become certified in PCI-DSS and ISO 27001. Here-in-After the internal auditor will address the risk, recommendations, risk Level, mitigation plan, implementation timeline, residual risk, monitoring & review.

AUDIT FINDINGS OBSERVATIONS AND RISK ASSESSMENT

1. Network Security Deficiencies

1.1. Outdated firewall rules

- **Observation:** The audit revealed that firewall rules are not regularly reviewed during a firewall audit at the Bank. Because as a result, the auditor found unused and overly permissive rules still continuing processing in the system. leaving potential entry points for unauthorized access.
- **Risk impact to the banking operations:** Outdated firewall rules could allow attackers to exploit vulnerabilities, gaining unauthorized access to sensitive banking applications. This could interrupt or damage online banking services, expose customers' and users' data to the 3rd parties (e.g.: user's passwords account details), and lead to financial fraud, reputational damage, and regulatory penalties due to resistance with compliance standards like PCI-DSS. If an attacker gain access that can lead IT operations to face long downtime period during business hours.
- **Recommendation:** implement missing firewall rules and remove unused or over permissive rules. Assign a senior level IT security officer to oversee this process, and ensuring rules align with current security policies and needs, also should monthly reviews by the SOC to monitor effectiveness of the firewall rules.

1.2. Unpatched systems and servers

- **Observation:** Several critical vulnerabilities were found and identified on internal servers due to unpatched software and outdated operating systems. The lack of updates leaves the systems to expose to known exploits and vulnerabilities that attackers could use to penetrate the bank's network.

- **Risk impact to the banking operations:** Unpatched servers and software could be compromised. that can lead to data breaches, some service outages (e.g.: ATMs or online banking), and data theft of sensitive customer information (PII) and credit & debit card details. This would interrupt IT operations, gain financial losses from fraud, and reputational damage to the bank, potentially violating ISO 27001 and PCI-DSS compliance.
- **Recommendation:** Apply critical security patches immediately and establish a patch management policy. The IT Operations should ensure servers are updated within 0-3 months, with monthly vulnerability scans to verify compliance. Also, can implement automation to the server updates.

1.3. Lack of network segmentation

- **Observation:** The auditor found out that there was no segmentation between internal and external network, that allowing unrestricted movement across the bank's network. This increases the risk of lateral movement if a cyber attacker breaches the perimeter.
- **Risk impact to the banking operations:** A lack of segmentation could enable an attacker to access critical systems like (e.g.: payment processing). From a less secure entry point, an attacker can gain access to whole system and lead to widespread disruption of banking services, data theft, and extended IT recovery efforts.
- **Recommendation:** Implement within 3-6 months network segmentation like VLAN to isolate internal and external traffic. The SOC team should ensure segmentation remains effective.

2. Weak Access Controls

2.1. Excessive privileged access

- **Observation:** Many of the employees in the bank system have administrator-level access to critical systems without a reason, violating the principle of least privilege. This can increase the risk of insider threats or accidental misuse.
- **Risk impact to the banking operations:** Excessive privileged access could allow unauthorized changes in the banking systems, leading to data manipulation, data transfer, service disruptions, or fraud. If there is a compromised account with elevated privileges could corrupt the IT operations and grind down customer trust, affecting revenue.
- **Recommendation:** Implement Identity and Access Management (IAM) system and conduct a privileged access review and enforce least privilege principles within 0-3 months. The IT Service Management and Security (ITSMS) team should review access control audits monthly to maintain security.

2.2. No MFA on online banking

- **Observation:** Online banking and internal systems only rely on passwords. no Multi Factor Authentication service implemented. that making them highly vulnerable to credential theft via phishing or brute-force attacks.
- **Risk impact to the banking operations:** Without MFA, attackers could easily access customer accounts by guessing passwords or phishing or brute-force attacks. that leads to financial fraud, loss of customer funds, and reputational damage. IT operations would face increased incident response costs, and the bank could face legal and regulatory consequences for inadequate security.
- **Recommendation:** implement MFA for all systems and internal users within 3-6 months with ongoing monitoring and testing to ensure effectiveness.

2.3. Inactive user accounts

- **Observation:** Inactive user accounts of former employees remain active in the bank network, and there is no process or an option to disable or terminate their account. that create opportunities for unauthorized access.
- **Risk impact to the banking operations:** Inactive user accounts could be exploited by former employees or attackers, that can lead to data breaches or illegal transactions. This could disrupt and compromise banking services, breaking down customer trust and bank reputation, also causing law enforcement impact because of violating compliance requirements.
- **Recommendation:** Implement automated account deactivation for terminated employees after they resign from the job within one month. Human Resources (HR) should manage this by reviewing user accounts to ensure there is no inactive users in the system.

3. Endpoint & Workstation Security Risks

3.1. No centralized Endpoint Detection & Response (EDR)

- **Observation:** The bank doesn't have an Endpoint Detection and Response solution to monitor the user activities, this issue leaves workstations without advanced threat detection or response capabilities to counter malware or insider threats.
- **Risk impact to the banking operations:** Without EDR, experienced attacks could go undetected to the current anti malware solutions. This can lead to disrupting workstation functionality, compromising customer data, and halting banking operations. Because of this IT operations would struggle to respond to the malicious activities, increasing downtime of services and recovery costs.

- **Recommendation:** Deploy an EDR solution like “CrowdStrike” across the network and deploy anti-virus software across all over the workstations within three months. The Windows/Mail/AV Team Lead (WMATL) should oversee this issue and daily EDR alert monitoring by the SOC team.

3.2. Missing security patches & antivirus updates

- **Observation:** Many workstations have outdated antivirus software versions and missing Windows critical security patches that can expose them to common malware and exploit targeting known vulnerabilities.
- **Risk impact to the banking operations:** Unprotected workstations could become entry points for ransomware, spyware or a zombie for a DOS attack. That could disrupt or unavailable the banking services, leaking sensitive data, and requiring broad IT remediation. This could lead to financial losses and reputational harm.
- **Recommendation:** Automate patch management and antivirus updates within 0-3 months. The WMATL team should implement this, with monthly endpoint vulnerability scans to verify essentials updates.

3.3. Use of unauthorized devices

- **Observation:** Employees use their personal USB drives and external hard disk devices without authority. This increases the risk of malware infections into the bank’s network.
- **Risk impact to the banking operations:** Unauthorized devices could infect systems with malware, that leading to data breaches, service outages, unwanted processing in the system and financial fraud. IT operations would face significant and unnecessary elimination efforts, that impact on quality of customer service and compliance.

- **Recommendation:** Enforce a device control policy to block unauthorized USB and external devices. Also block and add Active directory policy to restrict the USB ports of all the internal devices. Conduct regular device usage audits and create an EDR alert system to trigger alarm when an outside device gets plugged into the internal system.

4. Web & Application Security Gaps

4.1. Unsecured APIs

- **Observation:** the APIs that are used to connect apps and services do not use proper security measures. There's no strong authentication to check who's allowed to use them and no encryption to protect data in transit. Attackers could intercept or directly access sensitive banking data like customer info or transactions. This is a serious risk, especially in the banking system.
- **Risk impact to the banking operations:** Unsecured APIs could allow attackers to steal customer data or manipulate transactions, disrupting online banking and mobile services. This could lead to financial losses, regulatory fines, breaking customer trust and damaging IT resources.
- **Recommendation:** Implement API authentication mechanisms and API tunnel encryption mechanisms within 3-6 months. The Business Systems Support Operations Committee (BSSO) should manage this, with regular API security testing.

4.2. Weak input validation in web applications

- **Observation:** Online Banking services, input fields are vulnerable to SQL Injection and XSS (Cross-site scripting) attacks because of site developers didn't configure input validation inside the web applications.

- **Risk impact to the banking operations:** Attackers could exploit these vulnerabilities to compromise databases, gain access to customer accounts, alter data, or disrupt services, leading to financial fraud and downtime.
- **Recommendation:** Implement input validation and sanitization within 3-6 months. First identify all input points, define expected formats, validate inputs on both client and server sides, and sanitize inputs to remove potentially malicious characters. Do the penetration testing to verify the fixes.

4.3. Hardcoded credentials in source code

- **Observation:** Developers have embedded API keys and database credentials directly into the application source code, that making attackers to easily accessible if code is exposed to the outside.
- **Risk impact to the banking operations:** Exposed credentials could allow attackers to access critical systems and system databases, that can lead to data breaches, service interruptions, and fraud.
- **Recommendation:** Implement secure secret storage server solutions like “delinea secret server” to save credentials, should implement this within 3-6 months. regular code reviews to ensure compliance. Add encrypt security measures to the code.

5. Incident Response & Security Monitoring Deficiencies

5.1. Lack of documented incident response plan

- **Observation:** The bank has not documented formalized Incident Response Plan (IRP) in case of cybersecurity incidents, that leaving bank unprepared to handle cybersecurity incidents efficiently.

- **Risk impact to the banking operations:** Without an Incident Response Plan in case of incidents bank cannot handle threats or attacks, that causing prolonged service disruptions, data loss, and financial damage. IT operations would have to face delaying recovery process and confusion.
- **Recommendation:** Develop and test an Incident Response Plan within 3-6 months. Conduct an incident response drill every six months to improve the plan.

5.2. Limited security monitoring

- **Observation:** The entire SOC relies on manual log reviews of the servers and not configured any automated live monitoring system. Without having 24/7 live monitoring features, that limits the bank's ability to detect threats in real-time.
- **Risk impact to the banking operations:** Delayed threat detection could allow attacks to stay long inside the system and disrupt banking services create backdoors in the system to get back and compromising data. IT operations would have to face increased incident response costs.
- **Recommendation:** Deploy a Security Information and Event Management (SIEM) tool for real-time threat detection within 6+ months. SOC team should monitor the SIEM alerts every time it's triggered.

5.3. Delayed log retention

- **Observation:** Security logs files in the bank system are maintained for only three months, three months log files are insufficient for forensic investigations into past incidents.
- **Risk impact to the banking operations:** Limited log retention could hamper the incident investigation process, that can expose the bank to repeat same attacks. This could disrupt IT operations and violate regulatory requirements of audit procedure.

- **Recommendation:** Extend the banking system, all logs retentions to at least 12 months. ITOSU should do log retention audits every year. Also, should maintain backup of that 12 months old logs on an offsite.

6. Weak Third-Party Vendor Security

6.1. Unvetted third-party access

- **Observation:** Some third-party vendors have direct VPN access into the bank's internal network, but the bank hasn't done proper risk assessments on their access control. That could create potential risk of backdoors for attackers if the vendors compromised.
- **Risk impact to the banking operations:** Unvetted third-party access could lead to breaches into the system, disrupting services and leaking customer data. IT operations would have to make a lot of effort to isolate compromised systems.
- **Recommendation:** revoke all 3rd party access after establishing the system or service. Reauthenticate all the VPN access with the bank system. Also do or check annual 3rd party vendor security audits.

6.2. Non-compliance with security standards by third parties

- **Observation:** some third-party service and software providers fail to meet international standers like ISO 27001 and PCI-DSS standards when they build their productivity, and that can expose the bank to compliance risks.
- **Risk impact to the banking operations:** Non-compliant vendors could introduce vulnerable products to the banking system, that can lead to breaches that disrupt operations and malicious activities. This could damage customer trust because now a days business customers also check the banks are compliance with the international standards.

- **Recommendation:** Enforce ISO 27001 and PCI-DSS compliance with vendor contracts or get vendor support from those who have international standards. And do annual third-party compliance reviews.

7. Lack of Business Continuity & Disaster Recovery Preparedness

7.1. Unvalidated backup & recovery plan

- **Observation:** The Disaster Recovery Plan (DRP) that is used to survive in case of cyber-attack or sudden system breakdown, has not been tested in the past 12 months, that leaving the DR site effectiveness unverified and unstable.
- **Risk impact to the banking operations:** An untested DR site and DR plan could fail during a real incident, leading to extended outages of critical systems (e.g.: ATMs, online banking). That can lead to financial losses, and reputational harm. IT operations would face recovery delays and confusion.
- **Recommendation:** Document the entire DR plan and conduct a full DR drill and validate backup integrity within 6+ months. Also implement good backup strategy like 321 backup model. The Infrastructure Team Lead (ITL) should lead this, with annual DR testing and backup testing.

7.2. Insufficient redundancy

- **Observation:** There is no geographically separate backup site for critical systems in case of incident, that leaves the bank vulnerable to site-specific disasters.
- **Risk impact to the banking operations:** In case of a disaster like (e.g.: fire, flood) that could destroy the primary bank systems. Without redundancy, the bank has to face halting all critical banking services and causing significant financial and customer losses. IT operations would face extended downtime.
- **Recommendation:** Establish a geographically separate or cloud backup site within 6-12 months. And do annual testing on redundancy sites.

RISK ASSESSMENT PLAN

The risk assessment plan is here to summarize the risk, evaluate the risk level, and provide a summary of the mitigation plan to explain to the management.

NO	Identified Risk	Risk Level Evaluation	Mitigation / Treatment Plan	Monitoring & Review
01.	Outdated firewall rules	High	Implement annual firewall rule reviews, remove unused rules and add new rules.	Quarterly reviews by the SOC
02.	Unpatched servers	High	Apply stable critical security patches and implement patch management policy.	Monthly check updates and do vulnerability scanning
03.	Lack of network segmentation	High	Implement network segmentation (VLAN) to separate internal and external traffic.	Regular network traffic analysis by the SOC
04.	Excessive privileged access	High	Conduct a privileged access review and implement IAM system with the least privileged principles.	Monthly review access controls logins logs and time
05.	No MFA on online banking	High	Enforce multi-factor authentication for all customers.	Ongoing monitoring & testing of MFA function
06.	Inactive user accounts	High	Implement automated account deactivation for terminated employees.	reviews Quarterly user accounts and logins
07.	No centralized Endpoint Detection & Response (EDR)	High	Deploy EDR/XDR solutions that can access across all workstations.	Implement security and then monitor EDR alerts daily
08.	Missing security patches & antivirus updates	High	Automate to push patches through patch management and antivirus updates for all workstations.	Monthly check endpoint updates and scans
09.	Use of unauthorized devices	High	Enforce a device control policy to block unauthorized USB and external devices.	Monitor Regular device usage and restrict usb and other drives
10.	Unsecured APIs	High	Implement API authentication and API tunnel encryption mechanisms.	Regular API security testing

NO	Identified Risk	Risk Level Evaluation	Mitigation / Treatment Plan	Monitoring & Review
11.	Weak input validation in web applications	High	Implement input validation for bank applications to prevent SQL Injection and Cross-site scripting attacks.	Quarterly penetration testing
12.	Hardcoded credentials in source code	High	Implement secure secret storage server solutions.	Regular code reviews
13.	Lack of documented incident response plan	High	Develop and test an Incident Response Plan and conduct IR drill.	Annual incident response drills
14.	Limited security monitoring	Medium	Deploy SIEM for real-time threat detection.	SOC team monitors SIEM alerts
15.	Delayed log retention	Medium	Extend log retention to at least 12 months for forensic purposes.	Quarterly log retention audits
16.	Unvetted third-party access	High	Revoke 3 rd party vendor access after establishing their product.	Annual vendor security audits
17.	Non-compliance with security standards by third parties	High	Enforce ISO 27001 and PCI-DSS compliance also in the third-party vendor contracts.	Annual third-party compliance reviews
18.	Unvalidated backup & recovery plan	High	Conduct a full DR drill every 4 months and validate backup integrity and follow 321 backup model with incremental backup.	Conduct and testing a full DR drill every 4 months
19.	Insufficient redundancy	High	Establish a geographically separate backup site or cloud backup for critical systems.	redundancy stress testing in every 6 months

Table 1: Risk assessment plan for audit findings.

RISK TREATMENT PLAN FOR AUDIT FINDINGS

Note:

“Risk treatment plan for audit findings” created as a table structure in an excel file called "**Risk Treatment Plan For Audit Findings.pdf**" as a detailed version of risk treatment plan for Our Doha bank IT system.

AUDIT CONCLUSION

The cybersecurity audit of Our Doha Banks' IT system has identified several security gaps and non-compliance issues across critical areas of the bank IT infrastructure and also in the unethical security practices of the internal staff. These findings highlight significant vulnerabilities that could expose the bank system and services to cyber threats, financial fraud, and reputational damage. Specifically, the internal audit revealed weaknesses in network security such as outdated firewall rules, unpatched systems and servers, and a lack of network segmentation, weak access controls, including unnecessary privileged access for most of the users, and the absence of multi-factor authentication for online banking, and the existence of inactive user accounts. The audit also uncovered risks in endpoint and workstation security due to the lack of a centralized EDR solution, missing critical security patches and antivirus updates, and the use of unauthorized USB devices. In web and application security, the audit found unsecured APIs, weak input validation in web applications, and hardcoded credentials into source code. Additionally, there are absences in incident response and security monitoring, including a lack of a documented incident response plan, limited security monitoring capabilities, and lack of log retention. The audit also highlighted weak third-party vendor security due to unvetted access and non-compliance 3rd party products with no security standards. Finally, the bank demonstrates a lack of business continuity and disaster recovery preparedness with an unvalidated backup and recovery plan with insufficient redundancy. These identified gaps force to the urgent implementation of a comprehensive and robust risk treatment plan to mitigate the security risks and ensure compliance with industry standards such as ISO 27001 and PCI-DSS, as requested by the Board of Directors in the head of the bank.

MANAGEMENT RESPONSE

We acknowledge the findings from the cybersecurity audit and understand how important it is to fix the identified issues to protect our Doha Bank's data, IT infrastructure, and maintain customer trust, and meet regulatory requirements. We appreciate the detailed audit report from the internal audit team, and We fully support the recommended risk treatment plan and authorize all proposed corrective actions across the key audit areas, including Network Security, Access Controls, Endpoint Protection, Web and Application Security, Incident Response, Third-Party Vendor Management, and Disaster Recovery.

Management approves the necessary budget and resources for the implementation of all technical and non-technical improvements mentioned in the report. This includes the purchasing of required cybersecurity tools, such as EDR/XDR, SIEM, IAM systems, secure secrets storage like (delinea secret server), and any infrastructure needed for backup and recovery sites.

All the respective teams have been instructed to begin the perform as per the suggested timelines, with under supervision and progress reporting to senior management. This audit provides a clear path to enhancing our bank cybersecurity strength, and we are committed to ensuring timely and effective implementation.

Authorized by:

Chief Information Security Officer (CISO).

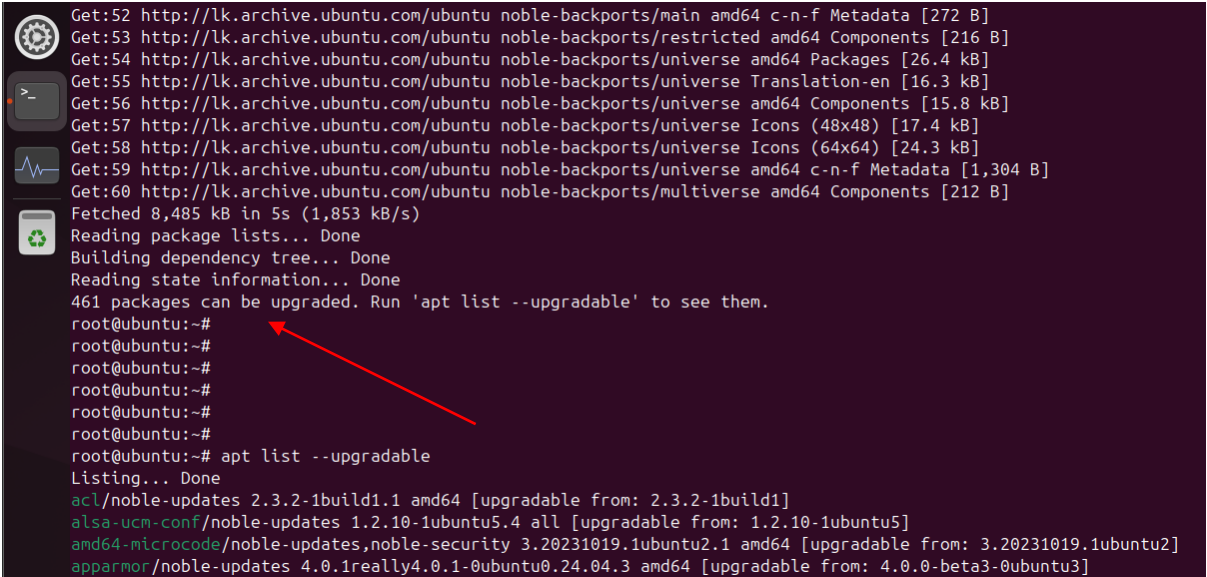
Board of directors.

Doha Bank

April 10th, 2025.

APPENDICES

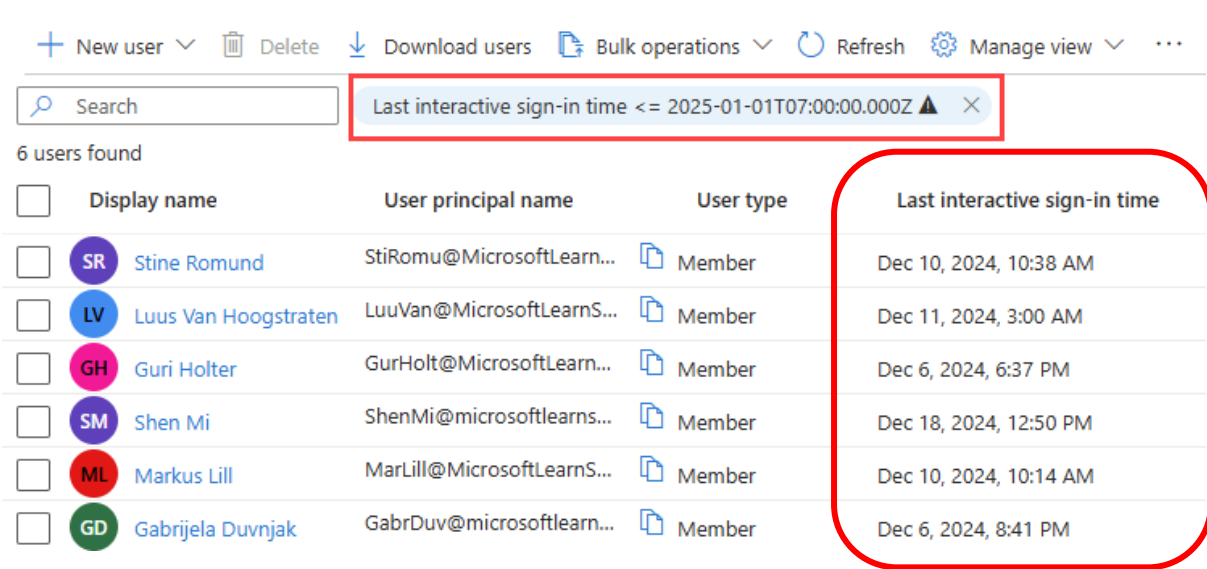
- Unpatched System Servers (Web Server-Ubuntu)

A terminal window showing the process of updating Ubuntu. It lists various components being fetched from the archive, including metadata, components, packages, translation files, and icons. After fetching, it reads package lists, builds a dependency tree, and reads state information. It then reports that 461 packages can be upgraded. The user runs 'apt list --upgradable' to see the list of upgradable packages. A red arrow points to the terminal output.

```
Get:52 http://lk.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [272 B]
Get:53 http://lk.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:54 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [26.4 kB]
Get:55 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [16.3 kB]
Get:56 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [15.8 kB]
Get:57 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe Icons (48x48) [17.4 kB]
Get:58 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe Icons (64x64) [24.3 kB]
Get:59 http://lk.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1,304 B]
Get:60 http://lk.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 8,485 kB in 5s (1,853 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
461 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~# apt list --upgradable
Listing... Done
acl/noble-updates 2.3.2-1build1.1 amd64 [upgradable from: 2.3.2-1build1]
alsa-ucm-conf/noble-updates 1.2.10-1ubuntu5.4 all [upgradable from: 1.2.10-1ubuntu5]
amd64-microcode/noble-updates,noble-security 3.20231019.1ubuntu2.1 amd64 [upgradable from: 3.20231019.1ubuntu2]
apparmor/noble-updates 4.0.1really4.0.1-0ubuntu0.24.04.3 amd64 [upgradable from: 4.0.0-beta3-0ubuntu3]
```

Figure 1: Unpatched System Servers (Web Server-Ubuntu)

- Inactive user accounts on the System

A screenshot of a user management interface. At the top, there are buttons for 'New user', 'Delete', 'Download users', 'Bulk operations', 'Refresh', and 'Manage view'. Below these is a search bar and a filter box that says 'Last interactive sign-in time <= 2025-01-01T07:00:00.000Z'. A table below shows 6 users found. The table has columns for 'Display name', 'User principal name', 'User type', and 'Last interactive sign-in time'. The 'Last interactive sign-in time' column is highlighted with a red rounded rectangle. A red box also highlights the filter box at the top.

+ New user ▾ Delete Download users Bulk operations ▾ Refresh Manage view ▾ ...			
🔍 Search			
Last interactive sign-in time <= 2025-01-01T07:00:00.000Z ⚠️ ×			
6 users found			
<input type="checkbox"/>	Display name	User principal name	User type
<input type="checkbox"/>	Stine Romund	StiRomu@MicrosoftLearn...	Member
<input type="checkbox"/>	Luus Van Hoogstraten	LuuVan@MicrosoftLearnS...	Member
<input type="checkbox"/>	Guri Holter	GurHolt@MicrosoftLearn...	Member
<input type="checkbox"/>	Shen Mi	ShenMi@microsoftlearns...	Member
<input type="checkbox"/>	Markus Lill	MarLill@MicrosoftLearnS...	Member
<input type="checkbox"/>	Gabrijela Duvnjak	GabrDuv@microsoftlearn...	Member
			Last interactive sign-in time
			Dec 10, 2024, 10:38 AM
			Dec 11, 2024, 3:00 AM
			Dec 6, 2024, 6:37 PM
			Dec 18, 2024, 12:50 PM
			Dec 10, 2024, 10:14 AM
			Dec 6, 2024, 8:41 PM

Figure 2: Inactive user accounts on the System

- **Missing security patches & antivirus updates on workstation computers**

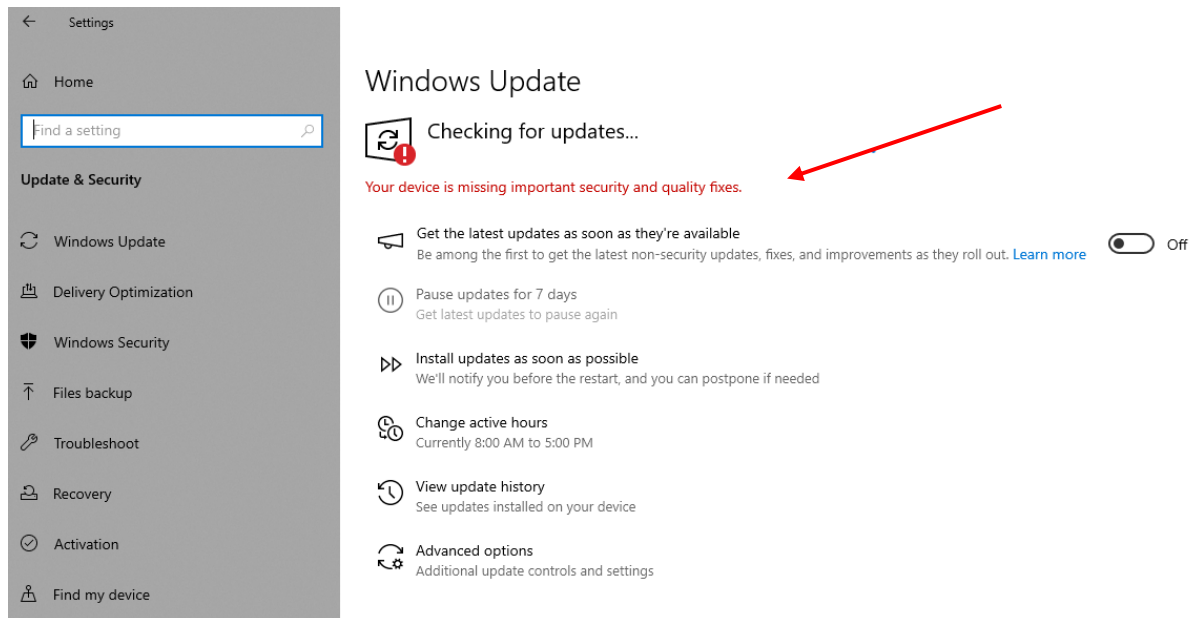


Figure 3: Missing security patches & antivirus updates on workstation computers

- **Nessus Vulnerability Scan Results on Servers**

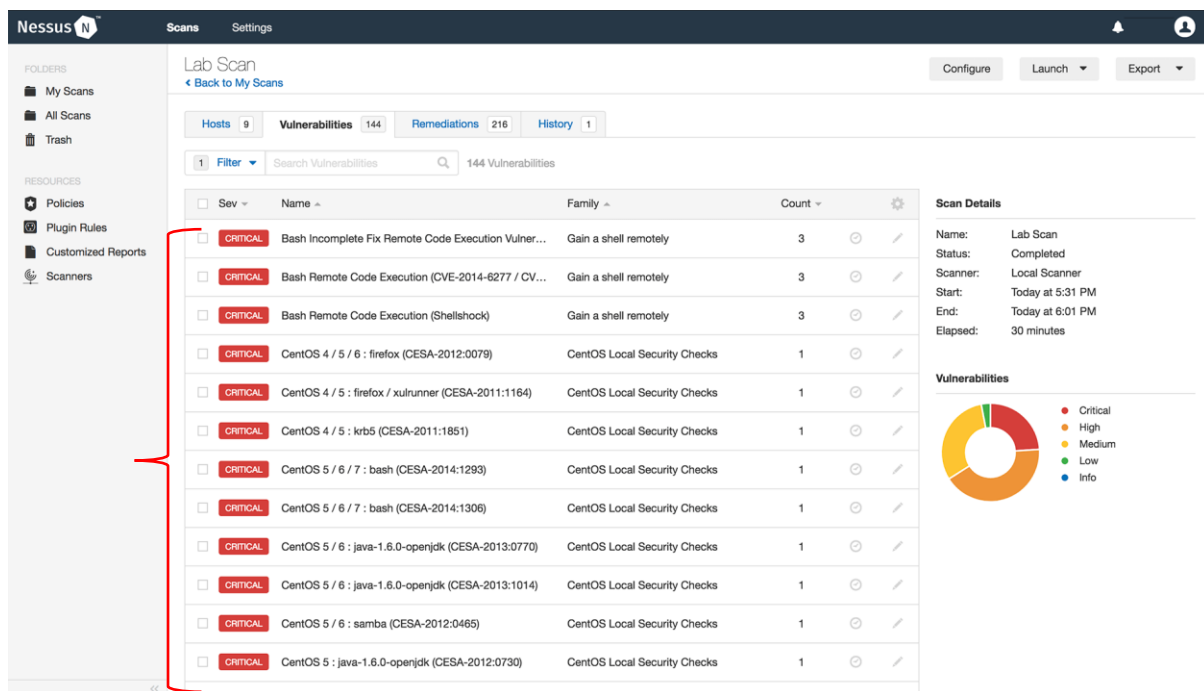


Figure 4: Nessus Vulnerability Scan Results on Servers

AUDITOR'S CERTIFICATION AND CONCLUSION

I, Devmith Subashana Jayathilake (Internal IT Lead Auditor), hereby certify this internal audit report is accurate and complete to the best of my professional knowledge and judgment. I take full responsibility for its findings and recommended solutions.

April 10th, 2025

.....

.....

Signature

Date

END OF THE AUDIT REPORT

REFERENCES

City of Fort Worth. (2021). *Cybersecurity audit report* (FY2021-5-7).

https://www.fortworthtexas.gov/files/assets/public/v/4/internal-audit/documents/fy2021/2021-5-7-cybersecurity-audit-report_final.pdf

Florida International University Office of Internal Audit. (2021). *Audit of university's IT*

network security controls (15-16-2). <https://oia.fiu.edu/wp-content/uploads/2021/06/Audit-of-Universitys-IT-Network-Security-Controls-15-16-2.pdf>

National Credit Union Administration Office of Inspector General. (2023). *OIG audit: NCUA*

cybersecurity (May 2023). <https://ncua.gov/files/audit-reports/oig-audit-ncua-cybersecurity-may-2023.pdf>

State of Colorado Legislative Audit Committee. (n.d.). *IT audit of cybersecurity resiliency:*

Public report (Audit No. 2250P). https://leg.colorado.gov/sites/default/files/documents/audits/2250p-it_audit_of_cybersecurity_resiliency_public_report.pdf

U.S. Department of the Treasury Office of Inspector General. (2024). *Treasury's*

cybersecurity information sharing (OIG-25-007). <https://oig.treasury.gov/system/files/2024-11/FY23%20Treasury%27s%20Cybersecurity%20Information%20Sharing%20%28OIG-25-007%29%20-%20508%20Compliant%20-%20SECURED.pdf>

AuditBoard. (n.d.). *4 key resources for effective audit reporting*.

<https://www.auditboard.com/blog/4-key-resources-effective-audit-reporting/>

The Institute of Internal Auditors. (n.d.). *Auditing report writing toolkit*.

<https://www.theiia.org/globalassets/site/auditing-report-writing-toolkit.pdf>

The Auditor General's Department, Sri Lanka. (n.d.). *PCA Chapter 08: English [Syllabus]*.

<https://aatsl.lk/images/pdf/syllabus/aa34-pca-chapter-08-english.pdf>

Leonov, A. V. (2016). *Nessus compliance results* [Image]. [https://avleonov.com/wp-](https://avleonov.com/wp-content/uploads/2016/12/NessusComplianceResults.png)

[content/uploads/2016/12/NessusComplianceResults.png](https://avleonov.com/wp-content/uploads/2016/12/NessusComplianceResults.png)

Microsoft. (n.d.). *Manage inactive user accounts in Microsoft Entra ID*.

<https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-manage-inactive-user-accounts?tabs=admin-center>

ClearTax. (n.d.). *Audit report*. <https://cleartax.in/s/audit-report>