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

Risk Treatment Plan For Audit Findings

NO	Risk	Risk Level	Mitigation Plan	Implementation Timeline	Residual Risk	Responsible teams/ parties	Monitoring & Review
01	**Outdated firewall rules**	High	Implement missing firewall rules and remove unused or over permissive rules. Assign a senior level IT security officer to oversee this process. Ensuring rules are align with current security polices and needs. Should monthly reviews by the SOC to monitor effectiveness of the firewall rules.	0-3 Months	Medium	ITSMS, ITOSU, CISU	Quarterly reviews by the SOC.
02	**Unpatched servers**	High	Apply / install critical security patches immediately. establish a patch management policy. Do monthly vulnerability scans to verify compliance. Implement automation to the server updates.	0-3 Months	Low	ITOSU, WMATL, ITL	Monthly check updates and do vulnerability scanning.
03	**Lack of network segmentation**	High	Implement VLAN network segmentation to separate internal and external traffic. The SOC team should ensure segmentation remains effective.	3-6 Months	Medium	ITSMS, CISU, ITOSU	Regular network traffic analysis by the SOC.
04	**Excessive privileged access**	High	Implement Identity and Access Management (IAM) system. Conduct a privileged access review. Enforce least privilege principles. The ITSMS team should review access control audits monthly.	0-3 Months	Low	ITSMS, MR, HR	Monthly review access controls logins logs and time.
05	**No MFA on online banking**	High	Implement MFA for all systems and internal users. Ongoing monitoring and testing to ensure effectiveness.	3-6 Months	Low	VPBS, ITSMS, PSTL	Ongoing monitoring & testing of MFA function.
06	**Inactive user accounts**	High	Implement automated account deactivation for terminated employees. HR should inform to the IT manage team to remove inactive users in the system.	0-3 Months	Low	HR, ITSMS, OA	Reviews Quarterly user accounts and logins.
07	**No centralized Endpoint Detection & Response (EDR)**	High	Deploy an EDR solution like “CrowdStrike” across the network. Deploy anti-virus software across all over the workstations. Daily EDR alert monitoring by the SOC team.	3-6 Months	Medium	ITSMS, WMATL, ITOSU	Implement security and then monitor EDR alerts daily.
08	**Missing security patches & antivirus updates**	High	Automate patch management and antivirus updates. endpoint vulnerability scans to verify essentials updates.	0-3 Months	Low	ITOSU, WMATL, ITL	Monthly check endpoint updates and scans.
09	**Use of unauthorized devices**	High	Enforce a device control policy to block unauthorized USB and external devices. Add Active directory policy to restrict the USB ports of all the internal devices. Conduct regular device usage audits in every six months. Create an EDR alert system to trigger alarm when an outside device gets plugged into the internal system.	0-3 Months	Low	ITSMS, ITOSU, MR	Monitor Regular device usage and restrict usb and other drives.
10	**Unsecured APIs**	High	Implement API authentication mechanisms. Implement API tunnel encryption mechanisms. Conduct regular API security testing.	3-6 Months	Low	VPBS, ITSMS	Regular API security testing.
11	**Weak input validation in web applications**	High	Implement validate inputs on both client and server sides, and sanitize inputs to remove potentially malicious characters. Do the penetration testing to verify the fixes.	3-6 Months	Low	VPBS, ITSMS	Quarterly penetration testing.
12	**Hardcoded credentials in source code**	High	Implement secure secret storage server solutions like “delinea secret server” to save credentials. Regular code reviews to ensure vulnerabilities. Add encryption methods to the code for security measures .	3-6 Months	Low	VPBS, ITSMS	Regular code reviews.
13	**Lack of documented incident response plan**	High	Develop and test an Incident Response Plan within 3-6 months. Conduct an incident response drill every six months to improve the plan.	3-6 Months	Medium	ITSMS, MR, ITSC	Annual incident response drills.
14	**Limited security monitoring**	Medium	Deploy a Security Information and Event Management (SIEM) tool for real-time threat detection. SOC team should monitor the SIEM alerts ever time it’s triggered.	6+ Months	Low	ITSMS, ITSC, VPITOPS	SOC team should monitors SIEM alerts.
15	**Delayed log retention**	Medium	Extend the entire banking system logs retentions to at least 12 months. ITOSU should do log retention audits every year. Maintain backup of 12 months old logs on an offsite.	12 Months	Low	ITSMS, ITOSU	Quarterly log retention audits.
16	**Unvetted third-party access**	High	Revoke all 3rd party access after establishing the system or service. Reauthenticate all the VPN access with the bank system. Check annual 3rd party vendor security audits.	0-3 Months	Medium	MR, BSSO, ITSMS	Annual vendor security audits.
17	**Non-compliance with security standards by third parties**	High	Enforce ISO 27001 and PCI-DSS compliance with vendor contracts. Get vendor support from those only who have international standards. Conduct annual third-party compliance reviews.	3-6 Months	Medium	MR, BSSO, ITSMS	Annual third-party compliance reviews.
18	**Unvalidated backup & recovery plan**	High	Document the entire DR plan and conduct a full DR drill. Validate backup integrity and implement good backup strategy like 321 backup model. Conduct / check annual DR testing and backup.	6+ Months	Low	VPITOPS, ITL, ITSMS	Conduct and testing a full DR drill every 4 months.
19	**Insufficient redundancy**	High	Establish a geographically separate or cloud backup site. Conduct annual testing on redundancy separate site.	6+ Months	Medium	VPITOPS, CISU, ITL	Redundancy testing and system stress testing in every 6 months.

Responsible teams/ parties’ identification name	
ITSC-	IT Steering Committee
CTSO-	Chief Technology and Services Officer
VPBS-	Vice President, Business Systems
VPITOPS-	Vice President, IT Operations
MR-	Management Representative
BSSO-	Business Support Services Officer
ITSMS-	IT Service Management and Security
ITOSU-	IT Operations Sub-Unit Head
CISU-	Communications and Infrastructure Sub-Unit Head
PSTL-	Payment Systems Team Lead
WMATL-	Windows/Mail/Antivirus Team Lead
ITL-	Infrastructure Team Lead
OA-	Office Administration
HR-	Human Resources