University of Central Lancashire
UCLan

Coursework Cover Sheet

Students should complete the input fields contained in this form and attach it in front of your formal assessment submission. All fields within this form are required. Please ensure that check boxes and radio buttons are appropriately selected. The last three questions are just for you to personally consider.

Department and assessment information:

School Name: School of Engineering and Computing

Assessment title: Risk Assessment Report

Course Title: Cyber Security
Module Title: Information Security Management
Module Code: CO2521
Year of Study: 2025

Academic Misconduct / Plagiarism Declaration

By attaching this front cover sheet to my assessment I confirm and declare that **I am the sole author of this work**, except where otherwise acknowledged by appropriate referencing and citation, and that I have taken all reasonable skill and care to ensure that no other person has been able, or allowed, to copy this work in either paper or electronic form, and that prior to submission I have read, understood and followed the University regulations as outlined in the Academic Integrity Policy and Procedure for Academic Misconduct

Have you checked the following? This will help your assessment achievement.

I have applied the learning outcomes for this module ☒
I have checked for Academic Integrity via Turn-it-in ☒
I have followed the guidance in the Assessment Brief and have not used AI to boost my grade unfairly. ☒
I have used references in accordance with instructions in the Assessment Brief ☒
I have proofread my work for spelling, grammar and punctuation. ☒
I have checked that the word count/size of this submissions accords with the guidance provided in the Assessment Brief. ☒

Well-being

We wish to support any student who is experiencing mitigating circumstances which prevents students from performing to the best of their ability when completing or submitting assignments. If you are experiencing such circumstances, then you may apply for Mitigating Circumstances. Wherever possible this must be done prior to handing in your assignment.

Do you need to apply for mitigating circumstances for this assignment Please select Yes / No

Please refer to the Mitigating Circumstances Policy

Questions you may wish to consider:

1. Have I allowed sufficient time to prepare this assessment?

2. Have I reflected on previous feedback and made improvements in accordance with advice?

3. What grade am I expecting?

1. Introduction

XYZ-VISA plays a critical role in managing visa applications and issuing. Importance of safeguarding the information stored by XYZ-VISA is paramount, as the nature of their work means that they have to keep personal information of all of their clients, which makes them a prime target for an attack from bad actors.

The subsequent sections of this report will cover the relevant security governance and laws in the context of XYZ-VISA, risk assessment, security controls involving assets as well as BYOD strategies, practical applications of security strategies with both hardware and software and finally relevant CVEs in the context of the threats identified.

2. Security Governance and Laws

2.1 The Importance of Cyber Security

Cyber Security threats are dynamic and constantly changing to become more sophisticated. The controls we use must do the same to remain effective. A security method implemented at a company's inception can quickly become obsolete as new attack vectors are discovered. This is why methods must be continually updated and monitored.

2.2 Security Governance in Cyber Security

"Cyber security governance is how you control and direct your organisation's approach to cyber security. When done well, it will effectively coordinate the activities of your organisation, when done badly it will lead to poor and delayed cyber security risk decision making (NCSC, 2023)"

Security governance should be done on a case-by-case basis, as there is no simple solution applicable to all companies. Within a company such as XYZ-VISA the focus should be aligning the strategies with their business objectives.

Security governance involves continuous reassessments to identify potential threats or vulnerabilities. Using these assessments to select security strategies, the company can prioritize mitigating risks that pose a larger threat to the company's operations. Two relevant standards to adhere to when developing this area would be ISO/IEC 27001 and ISO/IEC 27005:2022:

- 27001:2022 provides requirements for implementing, maintaining and improving an Information Security Management System (ISMS).

- 27005:2022 expands and provides further guidance on the implementation of the IS risk requirements specified in 27001:2022.

Security governance also includes the development and reassessment of security policies. By developing these policies in line with company goals it ensures they are relevant to the current state of the company's infrastructure. A relevant standard to be considered within this aspect would be the NIST Cybersecurity Framework (CSF) 2.0 as this framework contains resources to assist in the development as well as the reassessment of security policies.

Monitoring Security is crucial in security governance. Ensuring security controls are up to date, relevant, and not creating risks to the company. Unlike policy development, this involves the use of programs to monitor new threats and vulnerabilities on a wide scale and reduces human error. For this NIST SP-800-137 is useful, as it provides guidelines for Information Security Continuous Monitoring, giving strategies for implementing programs to monitor assets as well as associated threats and vulnerabilities.

Finally, in the development of all areas of security governance, UK law should be placed at the forefront, The UK General Data Protection Regulation (UK GDPR) for example, should be placed in significant consideration when developing policies for XYZ-VISA, as due to the nature of their business and the data they store there is always potential to make mistakes when implementing new governance.

3. IT Infrastructure

The overview of XYZ-VISA's internal IT infrastructure is as follows:
- Staff PCs running Windows 10
- A Microsoft SQL server database engine
- A Kerberos service that handles authentication of both staff and applicant accounts
- A Microsoft Exchange server that stores all emails and attached files
- A Microsoft Internet Information Service (IIS) web server, used for hosting XYZ-VISA's website for their applicants
- A D-Link DIR-878 firewall with firmware 1.12A1 to monitor and filter traffic/activity

4. Risk Identification

The identified assets, alongside their relevant threats and vulnerabilities, are listed below. Noting that two or more assets can cause a threat or vulnerability when used together.

Microsoft SQL Server Database Engine + Microsoft Internet Information Service Web Server
Threat - SQL Injection where a bad actor attempts to gain access to sensitive information or cause damage to the database.
Vulnerability - Improper input validation on the IIS web server before SQL queries are sent to the server.

Kerberos Authentication Service
Threat - Kerberoasting attack in order to gain an encrypted Kerberos ticket.
Vulnerability - Weak encryption of Kerberos tickets allows bad actors to easily crack the encryption and gain access to plaintext credentials.

D-Link DIR-878 Firewall with Firmware 1.12A1
Threat - Bad actors using command injection.
Vulnerability - Many firewalls are susceptible to specially crafted packages that can execute arbitrary commands to bypass security.

Microsoft Exchange Server
Threat - Email spoofing where a bad actor uses a forged sender address to disguise themselves and appear as if the email is legitimate.
Vulnerability - Improper or no validation of incoming emails means metadata can easily be changed prior to sending.

5. Risk Assessment

The relevant CVE's for each asset and their vulnerabilities have been considered in the context of XYZ-VISA. CVSS scores for each have been reassessed to reflect the risk they pose to XYZ-VISA.

The CVE's and their updated CVSS scores, in order of priority, are as follows:

Microsoft SQL Server Database Engine + Microsoft Internet Information Service Web Server - CVE-2024-28934

Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability
CVSS Version 3.x Base Score: 8.8 HIGH

This vulnerability allows a bad actor to execute arbitrary code due to certain inputs not being properly validated. This means a specially crafted request can be sent to the server in order to manipulate data or cause damage.

CVSS Version 3.x XYZ- VISA Updated Score: 9.2 CRITICAL

CVSS Updated Vector:
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:W/RC:X/CR:H/IR:H/AR:H/MAV:N/MAC:X/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H

This attack can theoretically be performed simply by accessing the website, requiring no credentials or interaction from an authenticated user, and the impact and requirement of the CIA triad are high across the board, causing the score to increase to 9.2.

D-Link DIR-878 Firewall with Firmware 1.12A1 - CVE-2019-8313

Command Injection Vulnerability
CVSS Version 3.x Base Score: 8.8 HIGH

This vulnerability is specific to DIR-878 running firmware 1.12A1 and allows a bad actor to perform command injection where arbitrary OS commands can be executed via a crafted /HNAP1 POST request by manipulating the request body of the SetIPv6FirewallSettings API function to send untrusted input to any HNAP API function.

CVSS Version 3.x XYZ-VISA Updated Score: 7.9 HIGH

CVSS Updated Vector:
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H

This vulnerability is specific to Firmware 1.12A1, and because updates to patch this vulnerability have been released since the CVE was published, Remediation Level can be changed to 'Official Fix' and Report Confidence can changed to 'Confirmed', which reduces the score to 7.9.

Kerberos Authentication Service - CVE-2022-33679

Windows Kerberos Elevation of Privilege Vulnerability
CVSS Version 3.x Base Score: 8.1 HIGH

This vulnerability allows a bad actor to perform a man-in-the-middle attack to downgrade the encryption of the targeted user's key to the RC4-md4 cypher, they can then crack the user's cypher key offline, gaining plaintext credentials for the user.

CVSS Version 3.x XYZ-VISA Updated Score: 7.6 HIGH

CVSS Updated Vector:
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C/CR:M/IR:M/AR:M/MAV:A/MAC:L/MPR:N/MUI:R/MS:U/MC:H/MI:H/MA:H

The risk score has decreased to a 7.6 due as a man-in-the-middle attack is unlikely to be performed unless the bad actor is on an adjacent network or in close proximity to the user. Additionally for the vulnerability to be exploitable the user must have 'Do not require Kerberos preauthentication' enabled and have a configured RC4 key, which are disabled by default.

Microsoft Exchange Server - CVE-2024-49040

Microsoft Exchange Server Spoofing Vulnerability
CVSS Version 3.x Base Score: 7.5 HIGH

A flaw in the verification process of the P2 FROM header causes non-RFC 5322 compliant headers to be allowed to pass through and be displayed by email clients, possibly exposing the company to malicious emails (e.g. phishing and malware)

CVSS Version 3.x XYZ-VISA Updated Score: 6.8 MEDIUM

CVSS Updated Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:F/RL:W/RC:R/CR:L/IR:M/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:H/MA:N

This exploit is a known issue across many email servers and services, functional exploits exist and work with minor modifications. However the method is well known and can be worked around by using services to properly authenticate incoming emails, so the score has decreased to a 6.8.

Performing this reassessment allows for risk mitigation to be prioritised based on factors that are relevant to the company, so that those that pose a larger threat can be dealt with first.

6. Security Controls

The following security controls are recommended to mitigate these risks and bring them within the acceptable risk appetite:

Security and Firmware Updates - Many services exist that are built to monitor and automatically update firmware and software. They are often highly customisable so that they may only update at certain times as to minimise disruption to availability. This prevents outdated and vulnerable firmware such as the case of the D-Link Dir-878 Firewall.

Email Verification - Similarly, there are many services such as Cloudflare that increase email security by providing protection from many different attacks, namely DDoS, Phishing and Spoofing attacks. This will help to mitigate risk associated with parts of the infrastructure such as the Exchange Server and IIS Web Server.

Strong Password Policies - Enforcing requirements such as a certain number of special characters, capital letters and numbers make passwords harder to guess, as well as increasing the difficulty of cracking them when, for example, encrypted credentials are acquired through a kerberoasting attack.

7. Bring Your Own Device (BYOD)

XYZ-VISA have requested additional assessment in order to allow employees to work with their own devices, this adds another attack vector and should be implemented with this in mind.

As BYOD places employee devices on the 'outside' of the IT infrastructure, it exposes them to the wider internet and eliminates the protection that security measures such as the firewall provides. This makes employees using BYOD susceptible to attacks, such as man-in-the-middle, that were previously not considered.

The following security controls along with their supporting technologies should be considered in the implementation of BYOD:

Device Management - Remotely monitoring devices that are using BYOD as if they were within the internal network. Administrators should be able to enforce policies and controls as if they were within the internal network. Mobile Device Management (MDM) as a supporting technology allows organisations to monitor and manage devices that their employees devices remotely.

Security Standards Enforcement - Enforcing security requirements on any device that attempts to remotely connect. This maintains the same security standards as the internal network. Network Access Controls (NACs) ensure connected devices meet the minimum security requirements (e.g. updated antivirus) before being allowed to connect.

Although this is similar to the previous control and technology, NAC assesses the security of the devices through authentication and access control, whereas MDM focuses on general management of the devices and the applications they can use.

Data Encryption - Given the nature of XYZ-VISA's data this is the most important control for maintaining confidentiality and integrity. Virtual Private Networks (VPNs) allow for encrypted, secure connections to the network from BYOD devices, allowing employees to work from unsecure networks while still being protected from potential attacks.

Device Security Monitoring - Similar to standards enforcement, this involves monitoring connected devices for suspicious activities both on the device itself and in network traffic. This is another layer of security from the internal network that can also be remotely enforced on BYOD devices. Endpoint Detection and Response (EDR) is used for the monitoring and analysis of endpoint activities, acting like a sophisticated firewall that monitors and detects suspicious activity to prevent it from affecting the network or the device.

Multi-Factor Authentication - This control prevents unauthorised access to the network via compromised BYOD devices. It involves using two or more factors to identify yourself: Something you know (e.g. passwords), something you have (e.g. authenticator) and something you are (e.g. fingerprint, face ID). Technologies such as authenticators, facial and fingerprint scanners are the supports for MFA, meaning if a device is compromised it is significantly harder for a bad actor to access the network.

Some of these controls seem similar and that is because they should all be used in unison in order to provide the most security to BYOD.

8. Conclusion

This report has aimed to assess relevant security governance and laws in the context of XYZ-VISA, perform a risk assessment with relevant CVEs in the context of the threats identified, discuss security controls involving assets and finally BYOD strategies.

The key findings of the report were the following:
-XYZ-VISA must develop a strong security governance to protect the company, as well as the IT infrastructure's security.
-Multiple vulnerabilities within the internal IT infrastructure that are likely to be the cause of the attacks.
-Many of these vulnerabilities can be fixed by implementing basic security controls that were detailed in section 6.
-XYZ-VISA is able to introduce a BYOD policy so long as the appropriate controls and supporting technologies are introduced alongside it.
-Due to the nature of XYZ-VISA's work these security controls must be routinely reassessed and updated.

This report highlights multiple glaring issues with XYZ-VISA's current infrastructure. Implementing the security controls recommended and following continuous monitoring them will allow XYZ-VISA to ensure the confidentiality, integrity and availability of their information.

9. References

Anon (2024). *Risk Management*. NCSC. Available at: https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance [Accessed 27 Jan. 2025].

Da Veiga PhD, A. and Eloff PhD, J.H.P. (2007). *An Information Security Governance Framework*. [online] Taylor & Francis, pp.361–372. Available at: https://www.tandfonline.com/doi/citedby/10.1080/10580530701586136 [Accessed 27 Jan. 2025].

Hofesh, B. (2022). SQL Injection Attack: Real Life Attacks and Code Examples. [online] Bright Security. Available at: https://brightsec.com/blog/sql-injection-attack/. [Accessed 27 Jan. 2025]

Umberger, H. and Gheorghe, A. (2011). *Cyber Security: Threat Identification, Risk and Vulnerability Assessment*. [online] Dordrecht Springer, pp.247–269. Available at: https://link.springer.com/chapter/10.1007/978-94-007-0719-1_13 [Accessed 28 Jan. 2025].

Malatji, M. (2023). *Management of enterprise cyber security: A review of ISO/IEC 27001:2022*. [online] IEEE Xplore. doi:https://doi.org/10.1109/CyMaEn57228.2023.10051114. [Accessed 28 Jan. 2025]

ISO/IEC 27001:2022. (2022). 3rd ed. [online] ISO, pp.1–17. Available at: https://www.iso.org/standard/27001 [Accessed 29 Jan. 2025].

ISO/IEC 27005:2022. (2022). 4th ed. [online] ISO, pp.8–26. Available at: https://www.iso.org/standard/80585.html [Accessed 29 Jan. 2025].

National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, [online] 2.0(29). doi:https://doi.org/10.6028/nist.cswp.29. [Accessed 29 Jan. 2025]

Dempsey, K., Shah Chawla, N., Johnson, A., Johnston, R., Clay Jones, A., Orebaugh, A., Scholl, M. and Stine, K. (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organisations*. [online] National Institute of Standards and Technology, pp.6–13. Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf [Accessed 30 Jan. 2025].

Shastri, V. (2023). *Kerberoasting Attacks*. Crowdstrike. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/kerberoasting/ [Accessed 01 Feb. 2025].

Morrow, B. (2013). *Network Security - BYOD security challenges: control and protect your most sensitive data*. [online] ScienceDirect, pp.5–8. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1353485812701113 [Accessed 12 Feb. 2025].

Aarness, A. (2025). *What is Endpoint Detection and Response (EDR)?* [online] Crowdstrike. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ [Accessed 12 Feb. 2025].

Ncsc.gov.uk. (2024). Multi-factor authentication for your corporate online services. [online] Available at: https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services. [Accessed 12 Feb. 2025]

Calias, S., Caoli, B., Padilla, R., Tum-en, J., Bacilio, K., Lyn, I. and Guaki, G. (2024). *THE IMPACT OF BYOD (BRING YOUR OWN DEVICE) ON NETWORK SECURITY: A LITERATURE REVIEW*. 1st ed. [online] Southeast Asian Journal of Science and Technology, pp.1–6. Available at: https://sajst.org/online/index.php/sajst/article/view/303/259 [Accessed 13 Feb. 2025].