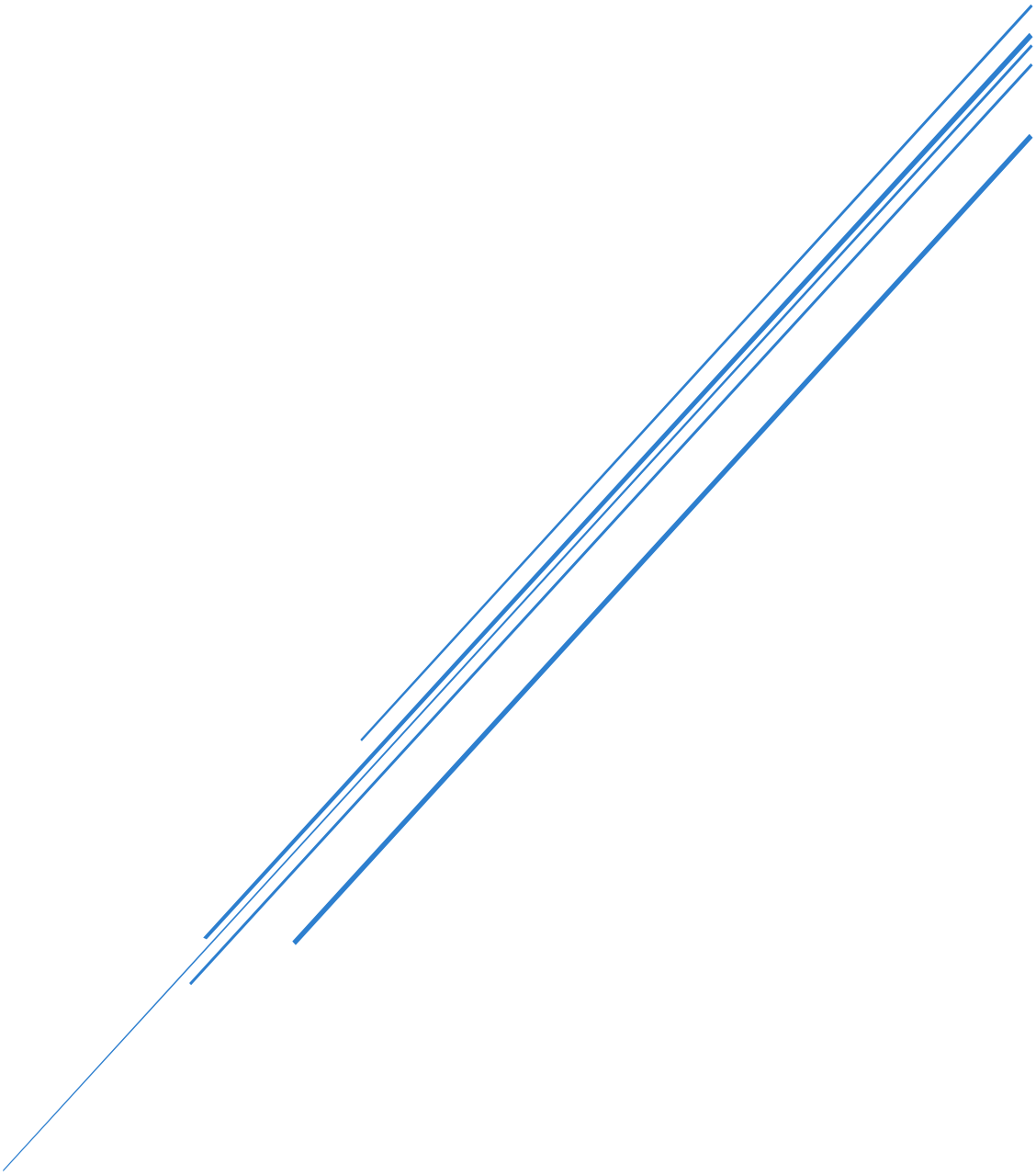
InnoVAR's Cybersecurity Risk & Compliance Report

Donna Naadu Botchway

Word Count: 2422



Robert Gordon University
23rd November, 2024

Table of Contents

1.0.Executive Summary

InnoVAR, established in 2016, provides of Virtual Reality (VR) and Augmented Reality (AR) services to industries like energy, construction, and government agencies such as the Ministry of Defence. With 300 employees and headquarters in Aberdeen, along with four global branches, InnoVAR operates in an industry where information security is critical. VR/AR projects deal with sensitive client data and intellectual property, which includes proprietary designs and extensive data sets like biometric, and behavioural data collected through user interactions. (Avey, 2024).

This report assesses InnoVAR's current information security posture by identifying risks, evaluating compliance with security standards, and recommending a security program to address the risks and achieve regulatory compliance. Highlighted in this document are key findings and recommendations with the analysis and proposed security program presented in an Excel file.

The risk assessment identified critical vulnerabilities such as outdated patches, weak access controls, insufficient testing and training, and poor backup practices. Threats found includes ransomware, data breaches, unauthorized access, data theft, and DoS attacks.

Gap analysis helps identify resource and security system gaps (Gregory, 2022). Using the NIST CSF standards to conduct the gap analysis highlighted several areas of non-compliance, particularly in governance, risk management, and recovery. Also included in this report is a security program with target state, clearly defined steps, roles, and timelines for each control measure, to address these challenges. Immediate focus should be placed on enhancing access controls, updating policies, training staff and developing a comprehensive incident response plan.

The security program designed actively supports InnoVAR's security strategy, ensuring alignment with its business goals and priorities (Gregory, 2022). Implementing the recommendations presented enables InnoVAR to meet the UK Ministry of Defence's requirements and attract clients who prioritize strong cybersecurity.

2.0. Risk Analysis

2.1. Overview

The risk analysis, documented in a risk register, identifies risks, threats, vulnerabilities, and current controls for InnoVAR's assets (Gregory, 2022). By assessing the risks, we aim to update processes and apply security principles that will bring InnoVAR closer to meeting the UK Ministry of Defence's Cyber Essentials requirements and strengthening its security posture (Kohnke, 2020).

2.2. Methodology

The assessment followed the NIST CSF framework, focusing on identifying assets, associated vulnerabilities, and potential threats. Key steps included:

2.2.1. Asset Identification: The risk analysis begins by identifying the assets of InnoVAR, a process needed in risk management and understanding the impact of potential threats on the assets (Kassa, 2017).

2.2.2. Vulnerability Analysis: After identifying assets, the vulnerabilities are assessed, focusing on weaknesses that could be exploited. This helps point out potential failure points and the controls needed to mitigate them (Mathenge, 2020).

2.2.3. Threat Evaluation: Potential actors, their capabilities, and the likelihood of targeting the assets is assessed. This helps prioritize risks and choose appropriate security measures (NIST, 2024c).

2.2.4. CAPEC and CVE Databases: To improve the analysis, the CAPEC and CVE databases were used. CAPEC provides a dictionary of attack patterns, while CVE records known vulnerabilities, to assist in identifying and addressing system weaknesses (MITRE, 2024).

2.2.5. Likelihood and Impact Assessment: The assessment used the metric below, categorizing likelihood from "Rare" to "Almost Certain" and impact from "Insignificant" to "Catastrophic," considering financial and other potential consequences. This combined scoring guides risk prioritization and response.

Overall Rating (L) X (I)	Likelihood (L)	Impact / Consequence (I)	
Critical > 20	(5) Almost certain	(5) Catastrophic	• Potential financial impact of one million pounds (£1,000,000) or more • Detrimental impact on operations or major projects • Sustained loss in reputation , • Life threatening • Sustained impact on services or quality • Regulatory non-compliance with probable litigation or penalties
High ≥ 13 & ≤ 19	(4) Likely	(4) Major	• Potential financial impact of five thousand pounds (£5,000) or more • Major impact on operations or major projects • Serious loss in reputation , • Extensive injuries, Regulatory non-compliance with probable litigation or penalties
Moderate ≥ 5 & ≤ 12	(3) Possible	(3) Moderate	• Potential financial impact of five thousand pounds (£5,000) or more • Moderate impact on operations or major projects • Short-term loss in reputation , • Regulatory non-compliance with potential to result in penalties
Low ≥ 3 & ≤ 4	(2) Unlikely	(2) Minor	• Potential financial impact of less than five thousand pounds(£5,000) • Minor impact on operations or major projects • No loss in reputation , regulatory non-compliance but unlikely to result in penalties
Very Low ≤ 2	(1) Rare	(1) Insignificant	• Potential financial impact less than 5 thousand pounds(< £5,000) • Impact can be absorbed by daily business running costs

Figure 1: Risk Metrics

2.3. Findings

For InnoVAR, critical risks are those that could lead to immediate or severe security incidents, such as data breaches, or significant disruptions in operations.

Based on the risk analysis, the table below highlights the assets, the vulnerabilities and threats identified.

Component	Assets	Vulnerabilities	Threats
Core Systems	Microsoft SQL Database Server, Microsoft Server, Microsoft Exchange Server 2019, Virtualized Windows Server 2022, Virtualized Servers	Outdated patches, Weak passwords, Inadequate encryption, SQL injection	Ransomware, Unauthorized access, Data breaches, Privilege escalation which could lead to the whole system being compromised
Data	Client Financial Data, Company Financial Data, VR/AR Source Code, Client Contact Details, Engineering Diagrams, Data Stored on Virtualized Servers	Inadequate encryption, Outdated information, Lack of data access control, Data storage and backup via USB, Lack of employee training	Intellectual Property theft, Data breaches, Information disclosure
Identity Access Management	Active Directory, Authentication Details	Weak access controls, Weak passwords, Poor account management (including delayed	Unauthorized access, Privilege escalation,

		account revocation), Inconsistent multi-factor authentication, Lack of employee training	Intellectual Property theft, Data breaches
Applications & Infrastructure	Application Server for VR/AR, VR/AR Application, Trend Antivirus, Third party Applications (Adobe, Java)	Lack of updates and outdated patches, Lack of encryption, Poor storage practices, Use of RDP by employees with admin privileges	Ransomware, Malware infection, Data breaches, Unauthorized access
Security Monitoring	Security Information and Event Management (SIEM)	Outdated rules	Failure to detect attacks
Network & Communication	Company VPN (Cisco AnyConnect), Gateway Router and Firewall (Cisco ASA 5525)	Use of shared default SSIDs and static passwords (Spartans2018), Misconfiguration or outdated firmware	Unauthorized access, Network security breach, Potential for lateral movement
Policies and Plans	Incident Response Plan, IT Policy	Outdated policy, Outdated procedures, Lack of testing and training, Poor employee awareness	Inadequate response to incidents, Prolonged downtime

2.4. Risk Register

The risk register captures the detailed results of the risk analysis, including the full list of identified risks, vulnerabilities, threats, corresponding risk ratings, and recommend controls for each. Please refer to the excel file for further details.

3.0. Gap Analysis

3.1. Overview

To develop a security strategy and achieve InnoVAR's objective to prove a minimum of cyber hygiene, a gap analysis was also conducted. This step clarified the current security posture of InnoVAR and identified areas for improvement, paving the way for achieving the objective (Gregory, 2022).

3.2. Methodology

The NIST Cybersecurity Framework (CSF) helps in implementing cybersecurity practices due to its comprehensive and flexible approach, especially in the VR/AR industry where sensitive data is heavily used. (Avey, 2024). By following NIST CSF, we evaluated the functions of Govern, Identify, Protect, Detect, Respond, and Recover. Compliance levels (Fully Compliant, Partly Compliant, Non-Existent, Unknown) were assigned based on alignment with the standard's requirements (NIST, 2024).

3.3. Findings

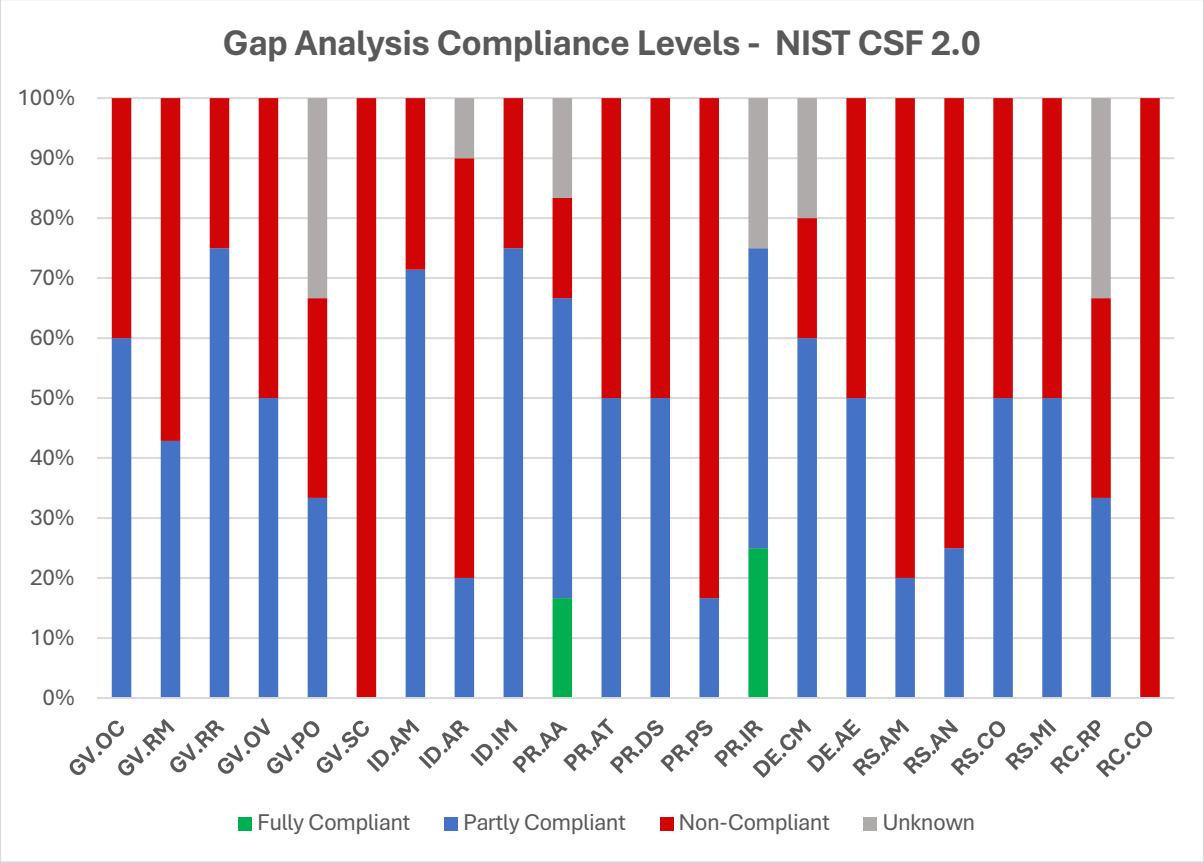


Figure 2: Gap Analysis Compliance Levels

Above is the graphical representation of InnoVAR's compliance status based on the gap analysis conducted. It highlights the areas of fully compliance, partial compliance, non-compliance and those with an unknown status. It shows that InnoVAR has several areas requiring attention to

achieve a minimum level of cyber hygiene. Below are the critical gaps that require immediate attention.

3.3.1. Supply Chain Management

InnoVAR has critical gaps in managing its supply chain with regards to security, particularly with third-party vendors for Adobe, AutoCAD, Java, the HR applications, Email spam filter, KPMG Spark, and relying on IT Works for incident response, vulnerability scanning and SIEM. Proper vetting and continuous monitoring of these vendors provides an understanding of their associated risks, which is essential to mitigate potential threats and ensure operational integrity (Campbell, 2014). Without these measures, InnoVAR faces increased risk of security incidents posed from third-party relationships (Cyber and Fraud Centre, 2024).

3.3.2. Risk Management

The security gaps found in InnoVAR show a lack of formal risk identification and management. The company relies on a part-time security employee among ten IT staff, all of whom juggle multiple responsibilities, while high-risk alerts are sent only to the IT director. This creates a single point of failure for incident response (Strawser, 2024) and highlights undefined roles. Although new employees receive a security awareness session, outdated policies and insufficient training leave staff unable to identify threats or secure sensitive VR/AR data. Relying on individual data owners for security is inadequate, as staff lack the necessary knowledge to prevent potential security risks (Robinson, 2024).

3.3.3. Incident Response

InnoVAR's incident response plan is outdated, with terminated employee contact information, which could hinder effective communication during incidents. Employees are neither trained nor aware of their specific roles in managing incidents. The absence of specific response or recovery tests nor training undermines the plan's reliability. According to Splunk, effective incident response requires preparation, role-specific training, and regular testing to ensure readiness (Splunk,2024). InnoVAR relies solely on its third-party provider, IT Works, for incident response, but there is no evidence of coordinated planning or collaboration between InnoVAR and IT Works. This limits InnoVAR's ability to address incidents effectively, leaving the company vulnerable to prolonged downtime, financial losses, and reputational harm (Cyber and Fraud Centre, 2024).

3.3.4. Identity and Access Management

The security gaps found in InnoVAR show inadequate identity and access management. Contractors are given unsupervised access, reflecting a lack of zero-trust practices. Generic password resets, a shared default SSID password, and a 90-day password change policy promote weak or reused passwords. Relying solely on passwords for account security is inadequate (Cyber and Fraud Centre, 2024), and multifactor authentication is inconsistently applied, with its use limited only to remote work. Remote employees have administrative privileges which pose risks of data theft or manipulation, especially given the lack of regular training (Cyber and Fraud Centre, 2024). Also, InnoVAR delays revoking access for terminated employees, as seen in a 2020 audit, which resulted in 10 former staff access. This issue likely contributed to two ex-employees joining a competitor and securing a key client, indicating potential misuse of sensitive company resources. These issues expose InnoVAR to insider threats and unauthorized access.

3.3.5. Vulnerability Management

InnoVAR's system updates and patches are inconsistently applied. This leaves servers, clients, and third-party software such as Adobe, Java, and AutoCAD vulnerable. Remote employees with local admin privileges store files on personal devices and USB drives, increasing the risk of malware and unauthorized access (Cyber and Fraud Centre, 2024). Trend Micro Antivirus is not automatically updated across the company. Monthly vulnerability scans are conducted by IT Works, but the SIEM application has not been updated with new rules since 2022. This prevents the InnoVAR from detecting emerging threats or addressing potential incidents in its environment, leaving it vulnerable to security risks (Gregory, 2022).

3.4. NIST CSF

The NIST CSF captures the detailed results of the gap analysis, including implementation examples, status, and notes to justify the status, grouped according to the functions. Please refer to the Appendix for further details.

4.0. Security Program

4.1. Overview

The security program detailed in the excel sheet, addresses gaps and risks identified in InnoVAR's operations. It aligns with InnoVAR's mission to provide VR/AR services to industries like energy and government. The program aims to support InnoVAR achieve Cyber Essentials certification to show proof of cyber hygiene and alignment with the NIST CSF (Gregory, 2022).

4.2. Methodology

The NIST Cybersecurity Framework 2.0 and the Cyber and Fraud Centre Scotland's guide served as a foundation to develop InnoVAR's security program. It addresses the gaps and risks identified during the analysis. The program includes clear milestones, responsibilities, and timelines, to be implemented over 12 months, with the IT Director leading, HR managing training, and Finance overseeing the budget. IT Works assists with vulnerability assessments, SIEM, and recovery tasks.

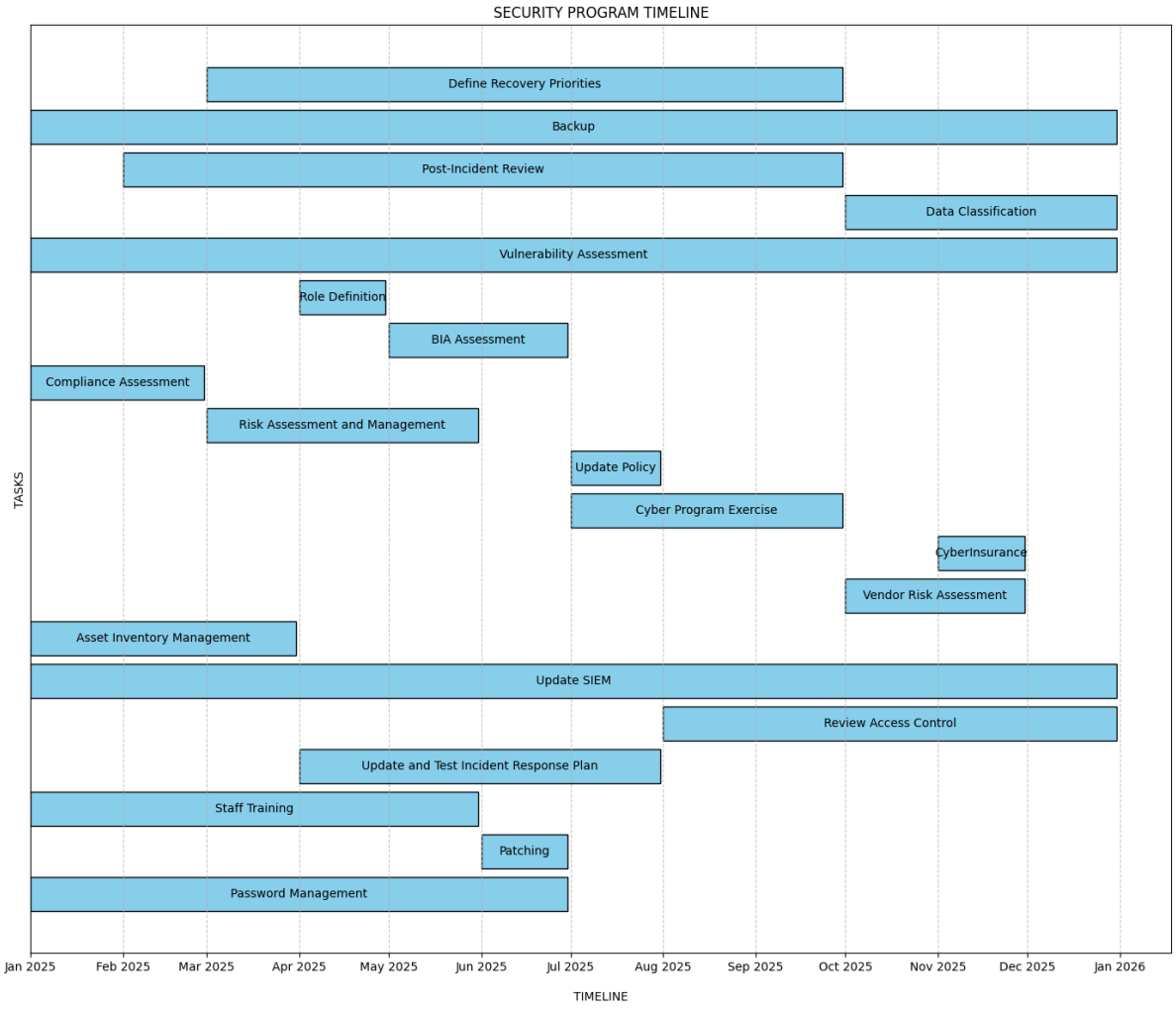


Figure 3: Security Program Timeline

4.3. Recommended Actions

The following actions address InnoVAR's critical risks and gaps. They are prioritized for immediate implementation due to urgency and feasibility, with additional recommendations in the appendix.

4.3.1. Patching and Updates

Patching is vital in addressing vulnerabilities. It ensures systems and applications are updated to prevent exploitation (Gregory, 2022). InnoVAR uses WSUS for Microsoft patches, however gaps remain in patching third-party applications and updating remote devices. To improve this process, the security program developed recommends automating patches and educating staff (Cyber and Fraud Centre Scotland, 2024).

4.3.2. Staff Training

InnoVAR’s security awareness program is limited to new employee sessions, with no ongoing training or tests. Bi-annual training should be implemented and linked to system access to ensure participation (Gregory, 2022). The security program covers how to train on key topics like password safety, phishing, and incident response.

4.3.3. Asset Inventory Management

InnoVAR's assets are informally tracked across branches. This poses risks of mismanagement. The security program provides guidance for maintaining a comprehensive asset inventory for devices, data locations, user accounts, and supplier-managed assets. The inventory should be updated quarterly to ensure accurate tracking and mitigate risks (Cyber and Fraud Centre Scotland, 2024).

4.3.4. Update Incident Response Plan

InnoVAR's incident response relies on IT Works, with an outdated plan and unclear roles, causing potential delays. The security program developed will help annually update the plan, define roles, and improve response through regular tests and training. Defining roles ensures personnel can confidently protect InnoVAR’s systems and data (Gregory, 2022).

4.3.5. Vendor Risk Assessment

In vendor risk assessment, the focus should not solely be on the degree of outsourcing but on ensuring proper due diligence in the outsourcing process (Gregory, 2022). InnoVAR currently relies on IT Works for vulnerability scanning and incident response and outsources HR applications and email spam filtering without sufficient due diligence. To address this, InnoVAR must annually assess and score vendor risks, develop mitigation plans, and monitor performance quarterly for effective risk management. (Kost, 2024).

4.3.6. Update SIEM

InnoVAR's outdated SIEM creates blind spots, leaving the organization vulnerable to undetected threats (Gregory, 2022). To mitigate this risk, InnoVAR must collaborate with IT Works to update the SIEM system and revise rules to cover emerging threats. Monthly reviews and updates should be performed, especially after significant IT changes (Pendello Solutions, 2024). InnoVAR's SIEM using threat intelligence and analysing data from multiple sources will reduce the risk of breaches and protect critical assets like servers (Pendello Solutions, 2024).

4.3.7. Review Access Control

The security program developed recommends limiting remote administrative privileges and immediate revocation of terminated employees' access to address InnoVAR's weak access controls. It also recommends supervising contractors' access and providing regular security training for remote staff. These measures aim to reduce the likelihood of unauthorized access, insider threats, and misuse of sensitive information at InnoVAR.

5.0. Conclusion

InnoVAR is positioned to significantly enhance its cybersecurity posture by implementing the developed security program to address the identified gaps and risks. The assessment highlighted concerns in incident response, patching, access controls, and vendor risk management. The current security posture of InnoVAR also suffers from insufficient staff training and outdated SIEM rules. This exposes the company to risks such as ransomware, data breaches, and insider threats.

The security program developed focuses on automating patching, bi-annual staff training, and updating the incident response plan to address InnoVAR's security gaps. It also prioritizes strong access controls, vendor risk assessments, and monthly SIEM updates. The security program outlined actions align with InnoVAR's goal of achieving Cyber Essentials certification and compliance with the NIST CSF standards. This supports InnoVAR's long-term security strategy as a VR/AR service provider handling sensitive data (Avey, 2024) and readiness to serve clients in highly regulated industries, including meeting the UK's Ministry of Defence Cyber Essentials requirements.

6.0. References

1. Campbell, G. (2014) *The Manager's Handbook for Business Security*. 2nd ed. Amsterdam: Elsevier.
2. Gregory, P. H. (2022) *CISM Certified Information Security Manager All-in-One Exam Guide*. 2nd ed. New York: McGraw-Hill.
3. Microsoft Security Response Center (MSRC) (2024) CVE-2022-41040. Available at: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 (Accessed: 21 October 2024).
4. CVE Details (2024) CVE-2024-43474. Available at: https://www.cvedetails.com/cve/CVE-2024-43474/ (Accessed: 21 October 2024).
5. CVE Details (2021) CVE-2021-26855: Microsoft Exchange Server Remote Code Execution Vulnerability. Available at: https://www.cvedetails.com/cve/CVE-2021-26855 (Accessed: 21 October 2024).
6. CVE Details (2024) CVE-2024-43474: Microsoft SQL Server Information Disclosure Vulnerability. Available at: https://www.cvedetails.com/cve/CVE-2024-43474/ (Accessed: 21 October 2024).
7. MITRE (2018) CAPEC 66: SQL Injection. Available at: https://capec.mitre.org/data/definitions/66.html (Accessed: 21 October 2024).
8. MITRE (2018) Exploiting Incorrectly Configured Access Control Security Levels. Available at: https://capec.mitre.org/data/definitions/180.html (Accessed: 21 October 2024).
9. Cisco Systems, Inc. (2022) Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability. Available at: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW (Accessed: 21 October 2024).
10. National Institute of Standards and Technology (NIST) (2019) CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability. Available at: https://nvd.nist.gov/vuln/detail/CVE-2019-0708 (Accessed: 21 October 2024).
11. Cloudflare (2024) 'What are the security risks of RDP? | RDP vulnerabilities'. Available at: https://www.cloudflare.com/learning/access-management/rdp-security-risks/ (Accessed: 21 October 2024).
12. National Institute of Standards and Technology (NIST), 2024. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide. Available at: https://doi.org/10.6028/NIST.SP.1300 (Accessed 04 November 2024).
13. National Institute of Standards and Technology (NIST), 2024. Cybersecurity Framework Profiles. Available at: https://www.nist.gov/cyberframework/profiles (Accessed 04 November 2024).
14. National Institute of Standards and Technology (NIST), 2024. NIST Cybersecurity Framework 2.0: Resource & Overview Guide. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf (Accessed 04 November 2024).
15. Yasar, K., Brush, K. and Crocetti, P. (2024) Disaster Recovery Plan. Available at: https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan (Accessed: 15 November 2024).
16. Cyber and Fraud Centre (2024) Cyber Strategy for Small Organisations. Available at: https://www.flipsnack.com/57FD8577C6F/cyber-and-fraud-centre-cyber-strategy-for-small-orgasniations/full-view.html (Accessed: 22 November 2024).

17. Avey, C. (2024) 'Exploring Security Risks in VR and AR', Tripwire, 14 November. Available at: https://www.tripwire.com/state-of-security/exploring-security-risks-vr-and-ar (Accessed: 22 November 2024).
18. Kohnke, A. (2020) 'The Risk and Rewards of Enterprise Use of Augmented Reality and Virtual Reality', ISACA Journal, Volume 1. Available at: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/the-risk-and-rewards-of-enterprise-use-of-augmented-reality-and-virtual-reality (Accessed: 22 November 2024).
19. Kassa, S. G. (2017) 'IT Asset Valuation, Risk Assessment, and Control Implementation Model', ISACA Journal, Volume 3. Available at: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model (Accessed: 22 November 2024).
20. Mathenge, J. (2020) 'Risk Assessment vs Vulnerability Assessment: How To Use Both', BMC Blogs, 27 May. Available at: https://www.bmc.com/blogs/risk-assessment-vs-vulnerability-assessment/ (Accessed: 22 November 2024).
21. National Institute of Standards and Technology (NIST) (2020) Security and Privacy Controls for Information Systems and Organizations. Available at: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (Accessed: 22 November 2024).
22. National Cyber Security Centre (NCSC) (2018) Updating Your Approach to Passwords. Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach#tip5-password-collection (Accessed: 22 November 2024).
23. National Cyber Security Centre (NCSC) (2024) Multi-Factor Authentication for Your Corporate Online Services. Available at: https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services (Accessed: 22 November 2024).
24. National Cyber Security Centre (NCSC) (2024) Response and Recovery Planning. Available at: https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-d/principle-d1-response-and-recovery-planning (Accessed: 22 November 2024).
25. Network Fish (2021) 'Security Risks When Using a USB Drive: All You Need to Know'. Available at: https://networkfish.com/pro-tips/security-risks-when-using-a-usb-drive/ (Accessed: 22 November 2024).
26. Walters, P. (2012) 'The Risks of Using Portable Devices'. Available at: https://www.cisa.gov/sites/default/files/publications/RisksOfPortableDevices.pdf (Accessed: 22 November 2024).
27. IASME (2024) Cyber Essentials Knowledge Hub: The Five Controls. Available at: https://ce-knowledge-hub.iasme.co.uk/space/CEKH/2563768794/The+Five+Controls (Accessed: 23 November 2024).
28. Robinson, P. (2024) 'Top 10 Data Security Measures Every Organization Should Have', Lepide Blog, 6 November. Available at: https://www.lepide.com/blog/top-10-security-measures-every-organization-should-have/ (Accessed: 23 November 2024).
29. Strawser, B. (2024) 'Understanding Single Point Failures: A Guide to System Resilience', Bryghtpath, 24 October. Available at: https://bryghtpath.com/single-point-failures/ (Accessed: 23 November 2024).
30. Pendello Solutions (2024) 'SIEM Implementation- Best Practices and Step-by-Step Guide'. Available at: https://www.pendello.com/blog/siem-implementation-best-practices-and-step-by-step-guide (Accessed: 23 November 2024).
31. Nduhiu, J. (2024) 'Incident Response Plans: The Complete Guide To Creating & Maintaining IRPs', Splunk Blog, 16 January. Available at:

https://www.splunk.com/en_us/blog/learn/incident-response-plans.html (Accessed: 23 November 2024).
32. Charboneau, T. (2021) 'Excluding Words Using Active Directory Password Policy', Infosecurity Magazine, 21 January. Available at: https://www.infosecurity-magazine.com/blogs/excluding-words-active-directory/#:~:text=Thankfully%2C%20Active%20Directory%20lets%20admins,how%20they%20may%20do%20so. (Accessed: 23 November 2024).
33. Kost, E. (2024) 'Implementing A Vendor Risk Assessment Process in 2024', UpGuard Blog, 18 November. Available at: https://www.upguard.com/blog/implementing-a-vendor-risk-assessment-process (Accessed: 23 November 2024).

7.0. Appendices

7.1. Appendix A

Risk Assessment Excel Sheet

Gap Analysis Excel Sheet

Security Program Excel Sheet