**InnoVar Security Consultancy Report**

**Rory Cameron Net Word Count: 2959**

Contents

[Executive Summary 3](#_Toc183690937)

[Risk Analysis 3](#_Toc183690938)

[Risk Register Metrics 3](#_Toc183690939)

[Assets 6](#_Toc183690940)

[Risks & Vulnerabilities 8](#_Toc183690941)

[Gap Analysis 12](#_Toc183690942)

[Security Programme 19](#_Toc183690943)

[References 20](#_Toc183690944)

# Executive Summary

Established in 2016, InnoVAR is a large engineering company specialising in the development of Virtual and Augmented Reality services for several industries, including energy, construction, and government agencies such as the UK’s Ministry of Defence (MOD).

To continue bidding for future contracts, the MOD has stipulated that InnoVAR must obtain a Cyber Essentials Certification from the National Cyber Security Centre (NCSC) and align its security programme with the ISO/IEC 27001 standard.

This report contains an analysis of the risks faced by InnoVAR, including a risk register outlining assets, vulnerabilities, threats, and risks derived from the provided case study. The report also includes a gap analysis of InnoVAR’s current security practices against the ISO/IEC 27001:2022 standard. Finally, a comprehensive security programme addressing the identified risks and gaps is provided. This programme is summarised in the report, outlining a one-year plan to achieve the NCSC Cyber Essentials Certification and align with the ISO/IEC 27001:2022 standard.

# Risk Analysis

Due to only having access to a InnoVAR case study, there may be assets not listed in the risk register, as well as any corresponding vulnerabilities of these assets. Furthermore, due to the limited technical information within the case study, there may be vulnerabilities that are not listed for known assets, or vulnerabilities that are already mitigated.

## Risk Register Metrics

A Risk Register was created based on the provided case study, detailing the risks InnoVAR faces, as well as the associated assets, vulnerabilities and threats of each risk. The layout of the Risk Register is as follows:

Risk ID

Identification of Risk

Asset

Valuable resource attempting to protect

Asset Value

A table with text on it

Description automatically generated

Figure 1 Asset Value Ranking

Asset Owner

Person(s) responsible for the asset

Vulnerability

A Flaw or weakness in an asset that can be exploited by a threat (Puzder, 2023)

Vulnerability Scale

A table with text and numbers

Description automatically generated

Figure 2 Vulnerability Ranking

Threat

Potential for a threat agent to exploit a vulnerability (Puzder, 2023)

Threat Scale

A table with text on it

Description automatically generated

Figure 3 Threat Value Ranking

Inherent Risk Likelihood

Risk Likelihood = Threat \* Vulnerability

Inherent Risk Impact

A table with text on it

Description automatically generated

Figure 4 Risk Impact

Inherent Risk

Inherent Risk = Likelihood \* Impact

Some risks are assigned a value different to the calculated value

A table with text and numbers

Description automatically generated

Figure 5 Risk Value Ranking

Current Controls

Already implemented controls in place to mitigate risk

Recommended Controls

Proposed controls to mitigate risk

Control Owner

Person(s) responsible for implementing and maintaining control measure

Date Due

Proposed control due date

ISO 27001 Reference

Reference to ISO 27001:2002 Annex a Control

Treatment Option

Mitigate, Transfer, Accept

Residual Risk Impact

See *Figure 4 Risk Impact*

Residual Risk likelihood

Residual Risk Likelihood = Threat \* Vulnerability

Residual Risk

Residual Risk = Threat \* (Vulnerability - Countermeasure) \* Residual Risk Impact

Next Review Date

Review of Risk and Controls

## Assets

The Risk Register has outlined **41 assets** derived from the case study, falling into 1 of 5 categories:

1. People
   1. InnoVAR employees and senior staff
   2. External contractors
2. Data
   1. Customer and company data
3. Intellectual Property
   1. Source Code and engineering diagrams
   2. IT/Password Policies and Incident Response Plan
4. Systems
   1. End point devices
   2. Servers (Web, Email, Database, Application, Storage)
   3. Applications
5. Property
   1. Offices and Data Centres
   2. Physical Security Systems (Passes, Turnstiles, Optical Readers)

Assets were given a value ranking based upon the value to InnoVAR (*Figure 1 Asset Value Ranking*).

A graph of a number of blue bars

Description automatically generated

Figure 6 Asset Worth Distribution Graph

|  |  |
| --- | --- |
| **Asset Value** | **Number of Assets** |
| **Very Low** | **0** |
| **Low** | **2** |
| **Medium** | **2** |
| **High** | **13** |
| **Very High** | **24** |

Figure 7 Asset Value Count

## Risks & Vulnerabilities

A graph of a number of bars

Description automatically generated with medium confidence

Figure 8 Distribution of Risks Graph

Derived from the InnoVAR case study, there are 159 total potential risks, detailed as followed:

|  |  |
| --- | --- |
| **Risk Value** | **Number of Risks** |
| **Very Low** | **0** |
| **Low** | **10** |
| **Medium** | **28** |
| **High** | **97** |
| **Very High** | **24** |

Figure 9 Risk Value Count

High Risk and Very High Risk areas means that there is a high likelihood of a threat exploiting a vulnerability of an asset, resulting in substantial impact for InnoVAR.

Vulnerabilities were ranked based upon *Figure 2 Vulnerability Ranking*, with Common Vulnerabilities and Exposures (CVE) ranked against the NVD CVSS, and then converted to *Figure 2 Vulnerability Ranking* appropriately.

The NVD CVSS (NIST, 2022)

A screenshot of a graph

Description automatically generated

Figure 10 CVSS Scoring System

In total there are **37 unique vulnerabilities**, ranging across all asset categories. There are **9** Critical vulnerabilities. These vulnerabilities should be addressed fist, as they pose the biggest threat to InnoVAR.

Critical Vulnerabilities

**Remote Local Administrator Access**

Employees using personal devices with local administrator capabilities while working remotely present a very high risk to the company due to the power granted to the device and individual. Having local admin privileges allow for the full controls over a device, including files, services and directories. A malicious threat agent exploiting this vulnerability could: disable endpoint antivirus, install malicious software, such as ransomware, pivot to other devices in the network to further an attack and generally weaponize the device to use against the company (SBS CyberSecurity, 2021).

The risk and likelihood of this vulnerability being exploited is extremely high, when considering potential threat agents. It was declared that InnoVAR recently had several laptops stolen from the office, as well as 10 ex-employees still having access to internal networks and applications. This puts the company at a very high risk of an attack, with implications being catastrophic and the potential for a total loss of InnoVAR services.

**Unsecured Data Stored**

Data is stored in a variety of locations, including an internal cloud architecture, local office file servers as well as locally on employee devices and USB drives. It is stated that it’s the data owner’s discretion whether to secure data, meaning there is likely sensitive company and customer data that is vulnerable. A malicious actor gaining access to this data could result in the introduction of ransomware, the public leaking of customer information, as well fraudulent activity from company and customer financial data.

This is very high risk to InnoVAR, due to the financial, legal and operational impacts data exposure would have. There have been 2 employees leave InnoVAR to work for its biggest competitor, where they recently gained a contract with one of InnoVARs main clients. This suggests that Ex employees have access to unsecured customer contact details and can use it in a malicious manner, advantages to them.

**Unrevoked Access**

As stated previously, it has been discovered that 10 ex-employees still have access to internal networks and applications, posing significant threat to the company and putting several assets at risk. Unrevoked access can result in the unauthorised access of data, compromising the CIA Triad, as well as access to servers and applications that would have a significant impact on the company’s ability to operate if tampered with.

**Repeated Password Across Networks**

There are 5 InnoVar offices which each have their own decentralized wireless network, as well as virtualized services used for file storage, printing and running applications. The vulnerability comes from the repeated use of the generic password “*Spartan2018*”, across all office networks.

By having a generic password that is not complex across all networks, if a malicious threat agent has gained the knowledge of 1 network password, through means of brute force attack, insider information from previous employees, they now know the password for all networks and can attempt to attack these too and gain unauthorised access. This puts InnoVAR at a very high risk from this vulnerability, having the potential to impact all services and operations.

**No Logical Access Controls from Office Network**

Whilst there is a separation between the office networks and live production networks, it appears that the production network is directly connected without any form of logical access control. This means that if there were to be an unauthorized access to any office network, the bad actor would also easily have access to the production network. From there they could carry out numerous attacks, such as data deletion and leaking as well as shutting down services and applications. Being connected to the production network, a bad actor may also have access to all other connected office networks.

**Repeated Password Used for Resets**

Password resets provided by the IT department are carried out the repeated password “*InnoVAR2020*”.

This vulnerability can be leveraged by numerous threats, such as ex-employees acting maliciously or on behalf of a competitor. By knowing the password, bad actors could exploit this vulnerability with social engineering, phishing or vishing to get an accounts password reset. From there a bad actor would be able to login as that account and gain unauthorized access. This poses a high risk to the company, due to the simplicity of the password, making it easy to brute force, as well as the potential impact that an unauthorised user would have within the company network.

**Outdated Incident Response Plan**

The Incident response plan was created in 2020 and last updated in 2022, meaning as of the time of this report (28/11/2024) it is 2 years out of date. The vulnerability here is that with having a response plan be out of date, new threats, risks and vulnerabilities may have been discovered that the response plan fails to address, as well as any policies or regulations that have been added that the response plan fails to meet. This poses a very high risk to InnoVAR, due to the potential for vulnerabilities to be exploited that the company has no documented mitigation methods for, as well as financial and legal repercussions the company might face, from either not meeting regulatory requirements, or for a successful attack against the company.

**No Response or Recovery Tests / Training**

The InnoVAR incident response plan fails to include response of recovery tests or training, stating that they rely on IT Works. The vulnerability here is that with a lack of testing or training, the overall effectiveness of mitigating an incident is critically low. Attackers can exploit this unpreparedness vulnerability to further damage InnoVAR systems, having a greater impact on the company, due to unpreparedness and lack of training.

**Terminated Employee Contact Information**

Terminated employees suggests some form of wrongdoing, where the employee may feel disgruntled and wanting to gain something back. The vulnerability exists where the ex-employees contact information is still listed on the incident response plan. This means that when there is an incident, they will be notified. This puts the company at a very high risk, as the ex-employee ma decide to act maliciously with this information, notifying competing companies, or other threat agents to further attack the company. They main gain insight into what the incident is and how it occurred, potentially beneficial information to an attacker. This vulnerability could increase the time taken for the incident to be resolved and the overall impact it has.

There are a further 22 vulnerabilities classed as “HIGH”, which should be mitigated next

1. Inadequate Security Awareness, Training and Education
2. Overburdened Employee
3. No Pass Holder Verification
4. Unsupervised / Trusted Contractor Access
5. Inadequate Physical Access Controls
6. No Physical Security Monitoring (CCTV)
7. No Secure Storage of Asset
8. Inadequate Password Policy
9. Missed Updates via WSUS
10. Legacy SharePoint Software Used
11. CVE-2019-1714 (Nist.gov, 2019)
12. CVE-2019-1708 (Nist.gov, 2019a)
13. CVE-2019-1715 (Nist.gov, 2019c)
14. Out of Date Versions Installed
15. Manual Updates Required
16. CVE-2019-1853 (Nist.gov, 2019d)
17. CVE-2021-34788 (Nist.gov, 2021)
18. Outdated IT Policy
19. Lack Of Continuous Employee Security Awareness, Training And Education
20. Lacks Up To Date Rules
21. Single Point of Failure
22. Third Party Reliance

# Gap Analysis

InnoVar has been asked to align their security program to the recognised ISO/IEC 27001:2022 Standard, which outlines controls for Information Security Management. Annex A contains 93 controls in 4 annexes:

A.5 Organizational controls

A.6 People controls

A.7 Physical controls

A.8 Technological controls

Numerous sub annexes have been omitted from this analysis, due to the lack of information provided in the case study, where reasonable assumptions cannot be made. There are [**Insert number controls here**]

The following table outlines the status metrics of controls:

A screen shot of a computer

Description automatically generated

Figure 11 Control Status Table

A5.1

The case study states that InnoVAR has some policies for Information Security, coming from a IT Policy, Incident Response Plan and Password Policy. Despite this, both the IT policy and incident response plan are outdated, as well as the password policy being inadequate in complexity and frequency. **Partially Compliant**

A5.2

InnoVAR has a dedicated IT team with 10 members split across company offices as well as an IT Director. InnoVAR only has 1 IT security employee, who is part time. **Partially Compliant**

A5.3

InnoVAR only has 1 IT security employee, who is also only part time. **Non Compliant**

A5.5

No contact with authorities described, simply with third party IT Works. **Non Compliant**

A5.6

No contact with special interest groups, simply with third party IT Works. **Non Compliant**

A5.7

Whilst InnoVAR doesn’t conduct threat intelligence, IT Works is a contractor which monitors potential threats on InnoVARs behalf. **Partially Compliant**

A5.9

No list of assets apart from the initial case study has been provided. **Non Compliant**

A5.14

Data is transferred using an internal cloud architecture, which consists of a Legacy SharePoint system and shared folders. The case study also states that InnoVAR has several office servers for office file storage**. Partially Compliant**

A5.15

External contractors have supervised and trusted access within offices. Remote employees have local admin privileges and ex-employees still have access. Active directory is in use for network management. **Partially Compliant**

A5.16

Passes are issued to contractors and visitors which are used in office turnstiles. **Partially Compliant**

A5.17

Once passes are issued, contractors generally trusted and unsupervised, very little verification done afterwards. **Partially Compliant**

A5.18

Contractors are generally trusted and unsupervised, employees have high level access rights when not necessary. . Active directory is in use for network management. **Partially Compliant**

A5.23

Active Directory in use for network management. **Partially Compliant**

A5.24

InnoVAR provides no training or preparation in incident management, and relies on third party IT Works. **Not Compliant**

A5.25

InnoVAR incident response plan has no response to incidents, and relies on third party IT Works. **Not Compliant**

A5.26

InnoVAR incident response plan has no response to incidents, and relies on third party IT Works. **Not Compliant**

A5.27

InnoVAR incident response plan has no recovery tests to incidents, and relies on third party IT Works. **Not Compliant**

A5.30

InnoVAR recovery plan is failover to unaffected offices, whilst in place does rely on at least 1 site being operational. **Partially Compliant**

A5.31

Prior to this report, from reading the case study InnoVAR does not meet MOD minimum requirements. **Not Compliant**

A5.35

No prior review taken place. **Not Compliant**

A5.36

No prior certification obtained. **Not Compliant**

A6.2

New employees are required to sign an acceptable user agreement and partake in a 30 minute security awareness presentation. **Partially Compliant**

A6.3

Employees receive an initial 30 minute security awareness presentation during onboarding, however no further training provided. **Partially Compliant**

A6.7

Remote employees required to use multifactor authentication and access network through a VPN, however remote employees have admin capabilities. **Partially Compliant**

A7.1

Optical turnstiles for passes for office entry and optical readers for data centre entry. **Partially Compliant**

A7.2

Offices have a reception desk, pass issuing process, and optical turnstiles. **Fully Compliant**

A7.3

Data centres have optical readers. **Fully Compliant**

A7.4

No form of CCTV. **Not Compliant**

A8.1

Password policy in place requiring 90 day change with complexity and at least 8 characters. **Partially Compliant**

A8.2

Admin Capabilities on remote devices. **Not Compliant**

A8.3

No policy on securing of data and files, down to employee discretion. **Not Compliant**

A8.5

Use of VPN and multifactor authentication. **Fully Compliant**

A8.7

SIEM, Vulnerability scanner, Antivirus and Firewall in use, how ever some applications are outdated **Partially Compliant**

A8.8

Same services from A8.7 **Partially Compliant**

A8.9

Generic common password used across office networks, default SSID names used. **Not Compliant**

A8.10

Ex employee contact information on response plan. **Not Compliant**

A8.12

Ex employees still have access to internal networks and applications, recent devices have been stolen from office and recent attacks. **Not Compliant**

A8.20

Default SSID used with common password “*Spartans2018*”. **Not Compliant**

A8.21

Default SSID used with common password “*Spartans2018*”. **Not Compliant**

A8.22

Production network connected to local office networks. **Not Compliant**

A8.31

Production Network is separated from test / office networks. **Fully Compliant**

A white sheet with black text

Description automatically generated

Figure 12 Annex A Company Compliance

A graph of different colored squares

Description automatically generated

Figure 13 InnoVAR ISO/IEC 27001:2022 Annex A Gap Analysis

# Security Programme

Outlined in the Security Programme is a 1 year time line that InnoVAR is suggested to follow to address the vulnerabilities and risks that they face. Due to time constraints, The Security Programme Does not show the proposed controls and countermeasures, how ever the risk register provides detailed recommendations to align with the ISO/IEC 27001:2002 Annex A controls.

The security programme first suggests addressing the critical vulnerabilities discovered. These are:

1. Remote Local Administrator Access
2. Unsecured data stored
3. Unrevoked ex-employee access
4. Repeated password across networks
5. No logical access controls from office networks
6. Repeated password used for resets
7. Outdated incident response plan
8. No response or recovery test / training
9. Terminated employee contact information

By addressing theses areas, InnoVAR can negate a significant amount of risk, having mitigated against technical vulnerabilities and implemented an IT policy, Password Policy and Incident Response Plan.

Rolling hiring of full time IT Security employees should be conducted, to mitigate against several vulnerabilities faced by having just 1 part time employee. This also allows for a more efficient delivery of the timeline and is aligned with several controls.

Technical vulnerabilities should be mitigated swiftly, A significant amount of InnoVARs technical vulnerabilities can be mitigated by conducting regular software updates, where these known vulnerabilities are patched.

Medium and Low vulnerabilities should be mitigated on a rolling basis after substantial amount of high risks mitigated.

Employee security training, awareness and education should be conducted every 3 months.

# References

NIST (2022). *NVD - Vulnerability Metrics*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln-metrics/cvss.

Nist.gov. (2019a). *NVD - cve-2019-1708*. [online] Available at: https://nvd.nist.gov/vuln/detail/cve-2019-1708 [Accessed 28 Nov. 2024].

Nist.gov. (2019b). *NVD - cve-2019-1714*. [online] Available at: https://nvd.nist.gov/vuln/detail/cve-2019-1714 [Accessed 28 Nov. 2024].

Nist.gov. (2019c). *NVD - cve-2019-1715*. [online] Available at: https://nvd.nist.gov/vuln/detail/cve-2019-1715 [Accessed 28 Nov. 2024].

Nist.gov. (2019d). *NVD - CVE-2019-1853*. [online] Available at: https://nvd.nist.gov/vuln/detail/CVE-2019-1853 [Accessed 28 Nov. 2024].

Nist.gov. (2021). *NVD - CVE-2021-34788*. [online] Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-34788 [Accessed 28 Nov. 2024].

Puzder, D. (2023). *Vulnerabilities, Threats, and Risks Explained | Office of Information Security | Washington University in St. Louis*. [online] informationsecurity.wustl.edu. Available at: https://informationsecurity.wustl.edu/vulnerabilities-threats-and-risks-explained/.

SBS CyberSecurity (2021). *The Danger of Local Administrative Privileges*. [online] sbscyber.com. Available at: https://sbscyber.com/blog/the-danger-of-local-administrative-privileges.