Information Security Management

By

Usiwoghene Ekebor

Table of Contents Page(s)

Executive summary

With the rate at which cybercrime is increasing annually, hackers are targeting high-value assets, Organizations such as InnoVAR must implement a strong information security framework to protect sensitive information, and to ensure business continuity with high value clients like the UK ministry of defence. The purpose of this report is to assess InnoVAR's security practices against the recommended ISO 27001 standard, with the aim of identifying vulnerabilities, risk assessment, and establishing strong controls to mitigate the potential threats. The ISO 27001 controls provide a guideline for organizations to build, implement and make continuous improvement of information security management (ISM).

The risk assessment performed from the available data, helped narrow down the main weaknesses in InnoVAR's IT assets and operations, which include vulnerabilities in Network Security, Identity and entitlements management, and intrusion detection and response planning. By applying the ISO 27001:2022 Framework, a compliance assessment was performed in the organizational, people, physical and technological security controls, with the aim to identifying areas where improvement would be needed. The report outlines a detailed one-year program for information security compliance that is divided into short term, medium term and long-term measures. Consequently, each task was matched with a security control and a metrics measuring the compliance progress and accountability. Furthermore, the security control implementation focuses on key areas, like the enforcement of access controls and improved monitoring of activity in the company's network. These steps could help InnoVAR mitigate risks, enhance compliance requirements while creating a security resilient culture at the same time.

Moreover, this report was put together by using secondary peer reviewed articles from Google Scholars and RGU Library and supported with information from verifiable web sources. Subsequently, InnoVAR compliance with ISO 27001:2022 security control goes far beyond satisfying the contract bidding requirements, it's also a proactive approach to information security goals.

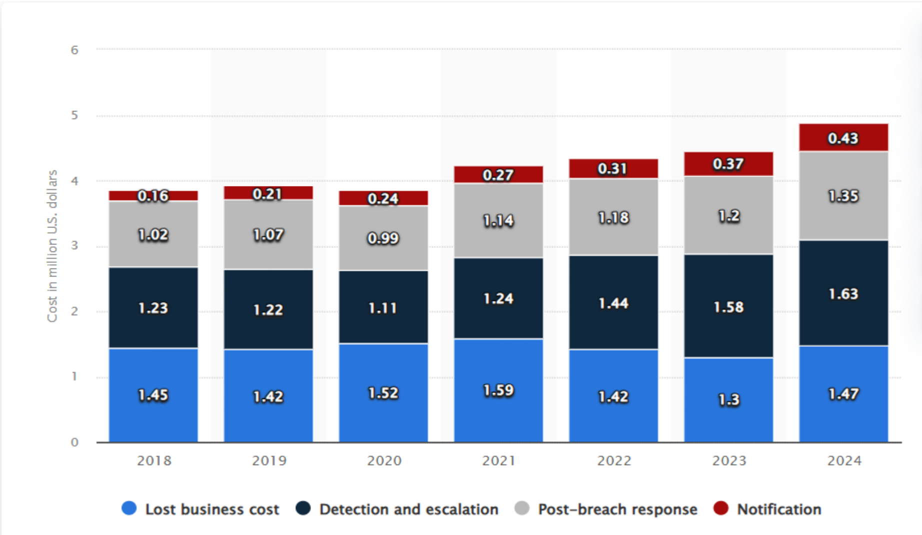
1.0 Introduction

Over the past several years the landscape of information security has been increasing due to the expanded use IT systems and the rapid growth in cyber threats. Initially, security was only just about physical and perimeter defences but with the sharp digital transformation, new challenges arrived which leads to the need of more robust measures. The release of ISO/IEC 27001 back in 2005 was a key milestone in the global standardization of Information Security Management (ISM) requiring a systematic, risk-based solution to protecting information (ISO/IEC, 2022). The standard has been updated since then and the 2022 version provided a strong control for modern threats, like cloud security and supply chain concerns.

An effective implementation of ISM offers companies a systematized way to address weaknesses, secure risks, and guarantee legal and regulatory compliance. Beyond threat mitigation, ISO 27001 promotes trust among stakeholders, improves operational efficiency and protects an organization's reputation. They emphasize that given the damage in terms of a data breach and ransomware attacks that cost business billions around the world, the need for ISM is more important than ever, with the average cost of breaches surpassing $4 million in 2024 (IBM, 2024).

InnoVAR is a technology-oriented company and is not an exception to these attacks, while trying to protect its assets and business operations the company is trying to comply with industry standards. This paper analyses these potential attacks and provides a guidline towards an improved security hygiene for compliance and attack mitigation. Furthermore, a strong ISM control like the ISO 27001 will ensure that InnoVAR reduces risks to its information and data, use assets more efficiently, and demonstrate the commitment to its clients.

Figure 1 Title Data breach worldwide from 2018 to 2024 by cost



Source Petrosyan Ani (2024)

2.0 Background

The history of information security can be traced back to the mid-20th century, during the Cold War the need to protect government sensitive and military data laid the foundations for secure systems and protocols to be created. In the beginning, this focused primarily on protecting physical assets and digital assets using basic encryption methods. Consequently, with the evolution of technology, security threats also evolved, and the paradigm shifted for how organizations approached the security of critical assists. Additionally, in the 1990s, when the internet was just starting to expand and cyberattacks were becoming common, the need for a standardized framework to help various organizations manage their information security arose.

Subsequently, the British Standard Institution (BSI), published BS7799, a formal standard for developing an Information Security Management System (ISMS) in 1998, which eventually became ISO 27001 (Gemserv 2017). This is where the ISO 27001 comes in, as it was introduced for this purpose back in 2005 as part of the ISO/IEC 27000 series. This standard was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to provide a framework for establishing, implementing and maintaining Information Security. ISO 27001 has evolved over time, with major changes occurring in 2013 and 2022 to meet emerging challenges including cloud computing and supply chain security (ISO 2022).

ISO 27001 and worldwide impact A measurable global impact of ISO 27001 Certifications Although the focus of this section is to analyses and be aware of the pros and cons of certified ISMS, certifiable ISMS such as ISO27001 are still widely considered globally. Certification of information security management system (ISMS) frameworks can indeed bring some perks: according to a Ponemon Institute (2022) study, organizations with ISM frameworks saved 27% in average data breach costs compared to those without certification. Moreover, compliance has increased consistently over time, with total numbers of ISO 27001 certificates issued worldwide exceeding 67,000 in 2021 (over a 20% increase since 2019) (CASCO 2024). The increase demonstrating that the standard works well in promoting trust, reducing exposure and mapping to best practices in managing information security risks.

3.0 Security Risk Assessment

A Security Risk Assessment (SRA) is a comprehensive process of identifying, assessing, and reducing risks of an organization’s assets. It ensures that the threats and vulnerabilities are detected so that appropriate controls can be implemented and resources allocated accordingly (Singh and Joshi 2018).

3.1 Identification of Assets

SRA starts with identifying assets, which is the collection of all resources vital to the organization’s functioning, that is hardware, software, data, human resources, and physical infrastructure. InnoVAR has those around the customer data Cloud Services, Data from IT devices, Proprietary Algorithms. This allows the company to determine the worth of these assets and the potential effect that they can have on business continuity if they are compromised. Repositories

3.2 Identified of Vulnerabilities

After identifying the assets, the next step is to determine weaknesses. Some common vulnerabilities are unpatched systems, poor access controls, poor configurations and lack of employee training. Other concerns at InnoVAR are potential device misconfiguration and lack of security guidelines in supplier management and operations, these vulnerabilities could result in data breaches, unauthorized access, or service disruption.

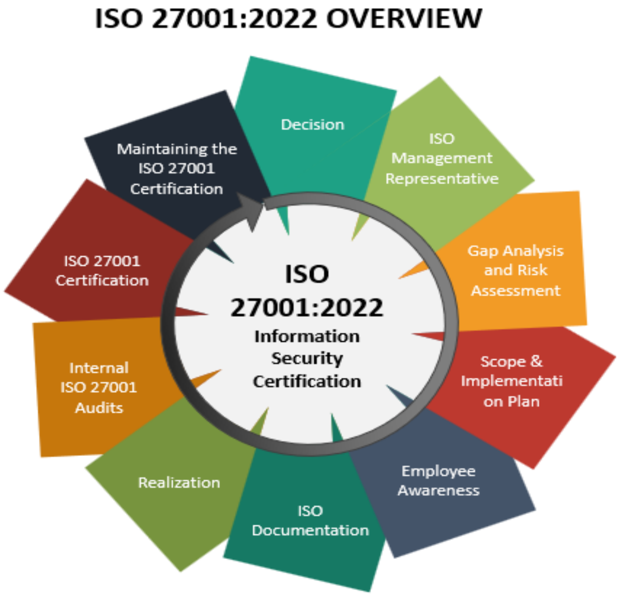
3.3 Risk Assessment Methodology

A qualitative risk assessment methodology that is in compliance with ISO 27001:2022 was used to assess InnoVAR. This means measuring risks by the probability and consequences which is classified as high, medium or low. The focus on risk prioritization guides the creation of a targeted security operation to reduce known weaknesses (ISO, 2022).

4.0 ISO 27001:2022 Information Security Controls Overview

The ISO 27001:2022 provides a strong basis for a well-structured control of information security. By implanting these controls at InnoVAR, four main areas were highlighted: People, Organizational, Physical, and Technological. The outcome is each domain contributing its strengths to the construct of assets integrity, confidentiality and availability.

Figure 2 Title Information Security Roles and Responsibilities


ISO 27001:2022 OVERVIEW
Decision
ISO Management Representative
Gap Analysis and Risk Assessment
Scope & Implementati on Plan
Employee Awareness
ISO Documentation
Realization
Internal ISO 27001 Audits
ISO 27001 Certification
Maintaining the ISO 27001 Certification
ISO 27001:2022 Information Security Certification

Source Shrinidhi Kulkarni (2024)

4.1 A5: Organizational Controls

Organizational controls lay the groundwork to properly derive information security. These control representations dictate governance structure and policy that guides the organization on how to protect the information assets.

4.2 A6: People Controls

The importance of people in implementing information security is emphasized through the people controls (A.6). By setting up regular trainings and awareness programs guarantees that safe practices must be enforced with employed individuals to minimize potential lapses created by human error. In addition, Proper employment termination procedures, like disabling access right when employees leave the organisation, also reduce insider threat risk. These controls help in improving the security culture of the organization.

4.3 A7: Physical Controls

Physical control is important for the protection of physical infrastructure where confidential information and critical systems are kept. Certain security measures, such as building physical security perimeters to create secured areas with barriers, surveillance, and restriction of access to key areas. These measures minimizes the risk of unauthorized access to physical assets and information, enhancing overall security of the organization.

4.4 A8: Technological Controls

Technological controls for cyber threats include all safety procedures that are put in place to protect digital systems and information. Regular backups ensure that data is available and intact should a system failure or cyberattack occurs, allowing for a quick restore of data. Additionally, security authentication actions like multi factor authentication (MFA) could tighten access control and prevent unauthorized system access. In this technology driven world, these security controls are essential in minimising cybersecurity risks.

5.0 InnoVAR Company Background: Security Practices and Compliance Level

InnoVAR is an engineering technology company with workforce of over 250 employees. The company specializes in Virtual and Augmented Reality (VR/AR) solutions for industries such as energy and construction, as well as government entities like the UK Ministry of Defence. The company's attitude toward security demonstrates a reactive rather than proactive approach despite its innovative portfolio.

5.1 InnoVAR Security Practices

The company’s security practices seem disorganised, with policies often instituted only when an identifiable threat arose, for instance, InnoVAR has adopted basic measures, such as antivirus software and firewalls, but there are no signs of the vulnerability programme being well maintained. There may be random trainings on cybersecurity, but the organization does not seem to have a culture of cyber security awareness. In addition, the absence of suggest monitoring mechanisms and comprehensive incident response strategies further suggests a critical deficiency in InnoVAR's capacity to prevent and address cyber risks efficiently. All of this shows how having a structured framework such as ISO 27001:2022 helps keep security practices independent of the human factor.

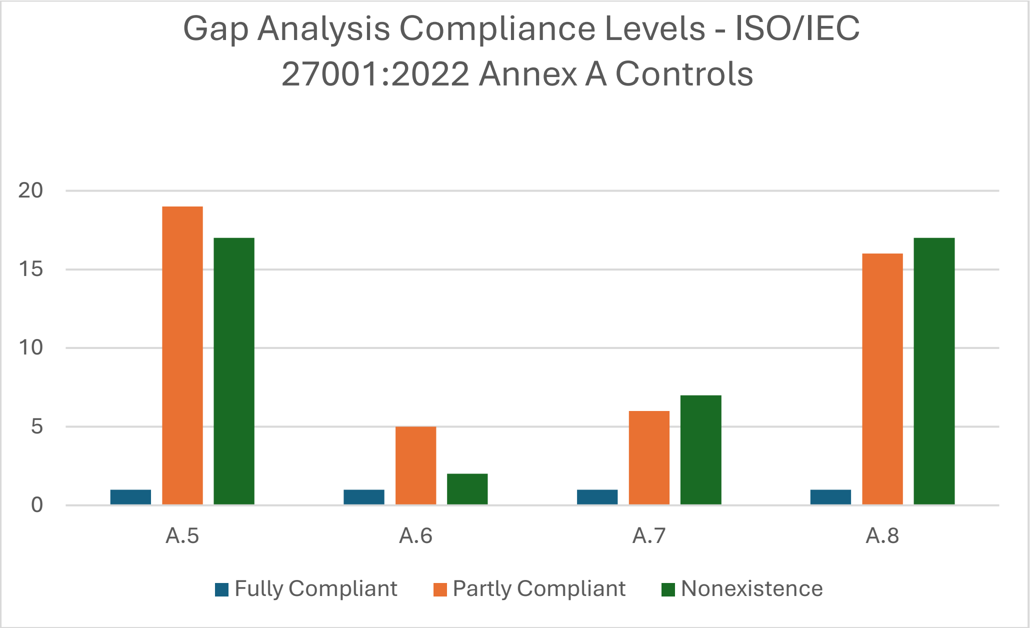
5.2 InnoVAR ISO 27001:2022 Compliance Level

InnoVAR is partial compliant with ISO 27001:2022, currently there are many gaps, both on organizational, as well as on the people control aspects. Some basic mechanisms like password policies, limited encryption protocols exist, but, weak areas include supplier relationship management, access control and implementation of formalized risk assessments. People control like adequate cybersecurity training for all employees and a clearly defined disciplinary structure for violators are weak at best, or non-existent. Also, the company is yet to institute a process for internal audits or independent reviews to assess compliance against established policies and procedures. These lapses reveal the gaps in InnoVAR’s alignment with ISO 27001:2022 as an essential measure to protect its business and stakeholders.

5.3 Gap Analysis Compliance Levels Graphical Representation

To visualize the compliance gaps, a graphical representation highlights InnoVAR's compliance level in the different information security control section and subsections. Bridging these gaps will necessitate targeted initiatives, such as enhancing supplier relationship security, formalizing people controls and conducting regular independent reviews to achieve the ISO 27001 certification.

Figure 3: InnoVAR ISO/IEC 27001:2022 Annex A Gap Analysis



Source InnoVAR Case Study (2024)

6.0 Security Program Development

The security program for InnoVAR is a high-level plan to reduce risk to promote accountability and compliance with ISO 27001:2022, and to also ensure that a good security is in place for the sections and subsections of organisational, people, physical and technological ISO 27001 controls. It was mapped to key tasks from the ISO framework which ensure that all controls are addressed systematically. The program was tailored to match InnoVAR's desires to increase their operational goals and improve resilience to the ever-changing cyber-attack landscape.

6.1 Task Overview and Structure

The security program is divided into different tasks, each of which is related to an ISO 27001:2022 domain: organizational, people, physical, and technological controls. Each task corresponds to specific control objectives, and collectively cover all vulnerabilities identified in the risk assessment.

6.2 Task Breakdown and Explanation

The tasks under the program are specifically designed according to InnoVAR's risk profile. Program tasks include detailed timelines, assignments of ownership and measurable outcomes, fostering accountability and efficiency.

6.3 Security Metrics

Metrics could be employed to measure the security program, such as, No. of security incidents that were resolved within predetermined thresholds, employee training completion rates and compliance audit scores. With the real-time tracking of such metrics, InnoVAR can gauge its progress and pivot as needed to counter new threat vectors and regulatory shortfalls.

7.0 Implementation Roadmap

The Implementation Roadmap for InnoVAR breaks down the execution of a scalable and sustainable security programme aligned to ISO 27001:2022 into phases. The roadmap organizes actions in order of urgency and where resources can be allocated, assuring an incremental progression towards complete information security and compliance objectives.

7.1 Short-term Actions (0-6 months)

The immediate focus is on addressing high-priority vulnerabilities and foundational controls. Key actions include developing and disseminating information security policies (A.5.1), initiating employee awareness and training programs (A.6.3), and implementing centralized logging and monitoring systems (A.8.15). Additionally, quick wins such as enforcing access control measures (A.5.15) and updating existing incident response plans (A.5.24) are prioritized to provide immediate risk mitigation.

7.2 Medium-term Actions (6-12 months)

This action period focuses on integrating more security controls and building processes that is sustainable. Tasks include enhancing redundancy mechanisms for critical systems (A.8.14), implementing secure development lifecycle practices (A.8.25), and conducting in-depth security testing for applications (A.8.29). Supplier risk assessments and contractual compliance measures (A.5.20) are also enhanced to secure external dependencies.

7.3 Long-term Actions (Ongoing)

The continuation of this phase will facilitate ongoing progress of InnoVAR's security posture. Periodic audits to address any further security concerns; employee training refreshers; and iterative changes for policies and procedures are performed. For example, advanced measures like the network segmentation (A.8. 22), and cryptographic standard improvements (A.8. 24), should be sustained to counter changing threats.

InnoVAR can incrementally and measurably make progress along this risk posture, compliance and operational resilience road map.

Conclusion

The report has rigorously assessed InnoVAR information security practices and gap analysis followed by a bespoke plan for successfully achieving compliance with the ISO 27001:2022 standard. The analysis underscores the pivotal role of systemic methodologies in effectively governing information security by showcasing the relevance of administrative, human, environmental, and techno-procedural safeguards in risk management and business continuity (ISO, 2022).

InnoVAR existing practices shows a foundational awareness of security needs, but there are gaps with respect to incident response, supplier risk, to name a few. A comprehensive security risk assessment was conducted to identify and map assets and vulnerabilities in line with best practices for risk reduction with high-impact risk areas prioritized for reduction. Laudon and Laudon (2022) states that a detailed security program, including specific tasks, metrics, and responsibilities, is a blueprint for achieving measurable improvements.

The implementation roadmap addresses risks in phases while laying out the groundwork for long-term sustainability. Prioritizes short-term action for very high vulnerabilities, medium-term action on integration and scalability and ongoing actions improves how to adjust to new threats (ISO, 2022)

Implementing these measures will enable InnoVAR to enhance its information security framework, safeguard critical resources, and exhibit adherence to global standards, building confidence with clients and stakeholders.

Recommendations

In short, for InnoVAR to acquires a solid Information security posture and with complete adherence to ISO 27001:2022 the following recommendations are suggested:

Establish a Security Awareness Culture - Training of staffs at InnoVAR should be provide continuously for security updates and awareness. Thes trainings should include a focus on how to identify phishing attempts and recognizing potential threats and vulnerabilities. Khando et al. (2021) states that that regular training can reduce human-related security incidents.

Incident Response and Business Continuity - Create and routinely test a full incident response plan and business continuity strategy. This must involve simulated cyberattacks to assess the InnVAR’s readiness. Effective incident response capability not only addresses impending threats but also minimizes financial and reputational impact (AL-Hawamleh 2024)

Strengthen Supplier Risk Management - Assess and verify compliance of supplier agreements with InnoVAR security requirements. Also, a periodic supplier audits and review of contracts that include terms and conditions requiring compliance with security policies should be conducted.

Enhance Technological Infrastructure - Implement updated monitoring solutions, like Security Information and Event Management (SIEM) tools, for real-time threat detection. In addition, mandate encryption for sensitive data, as well as implement multifactor authentication throughout systems. Also, New technologies such as AI-based anomaly detection could be implemented, which can tighten up existing defences (Chirra 2020).

Continuous ISO 27001 Compliance Evaluation - Perform an independent audit annually to find compliance gaps and remediate. This will also ensure the alignment with standards that continue to evolve, and regulatory requirements keeping InnoVAR's credibility with clients and other stakeholders.

References

AL-HAWAMLEH, A., 2024. Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems,* 15(1), pp. 1315–1331.

CASCO, 2024. *The ISO Survey.*

CHIRRA, D.R., 2020. AI-Based Real-Time Security Monitoring for Cloud-Native Applications in Hybrid Cloud Environments. *Revista de Inteligencia Artificial en Medicina,* 11(1), pp. 382–402.

GEMSERV, 2017. ISO/IEC 27001 and the General Data Protection Regulation (GDPR).

IBM, 2024. *Cost of a Data Breach Report 2024.*

ISO, 2022. *Information security, cybersecurity and privacy protection-information security management systems-requirements.* International Organization for Standardization/International ....

KHANDO, K. et al., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security,* 106, pp. 102267.

LAUDON, K.C., LAUDON, J.P. and TRAVER, C.G., 2023a. Essentials of Management Information Systems Fifteenth Edition Global Edition.

LAUDON, K.C., LAUDON, J.P. and TRAVER, C.G., 2023b. Essentials of Management Information Systems Fifteenth Edition Global Edition.

PETROSYAN ANI, 2024. *Cost distribution of data breach worldwide from 2018 to 2024, by main cost segments.* [online]. Available from: https://www.statista.com/statistics/1417524/worldwide-data-breach-by-main-cost-segments/

PONEMON INSTITUTE, 2022. *MANAGING RISKS & COSTS AT THE EDGE.*

SHRINIDHI KULKARNI, 2024. *ISO 27001:2022 - Control 5.2 - Information Security Roles and Responsibilities.* [online]. Available from: https://iso-docs.com/blogs/iso-27001-2022-standard/iso-27001-2022-control-5-2-information-security-roles-and-responsibilities

SINGH, U.K. and JOSHI, C., 2018. Comparative study of information security risk assessment frameworks. *International Journal of Computer Application,* 2(8), pp. 2250–1797.