

Evaluating ISO 27001's Impact on Organisational Cybersecurity: Benefits, Challenges, and Development of an ISMS Management Application

1. Introduction

In today's digital era, cybersecurity threats are increasing worldwide, making information security essential. ISO 27001 is a globally recognised standard which provides a structured, risk-based approach to managing information security. This project evaluates the impact ISO 27001 has on organisational cybersecurity.

2. Aim and Objectives

Aim: To evaluate the impact of ISO 27001 implementation in organisational cybersecurity by identifying the benefits and challenges of the implementation through real-world case studies.

Objective 1: To analyse the role of ISO 27001 in strengthening an organisational cybersecurity – Investigating how the standard enhances security measures, policies and controls within an organisation.

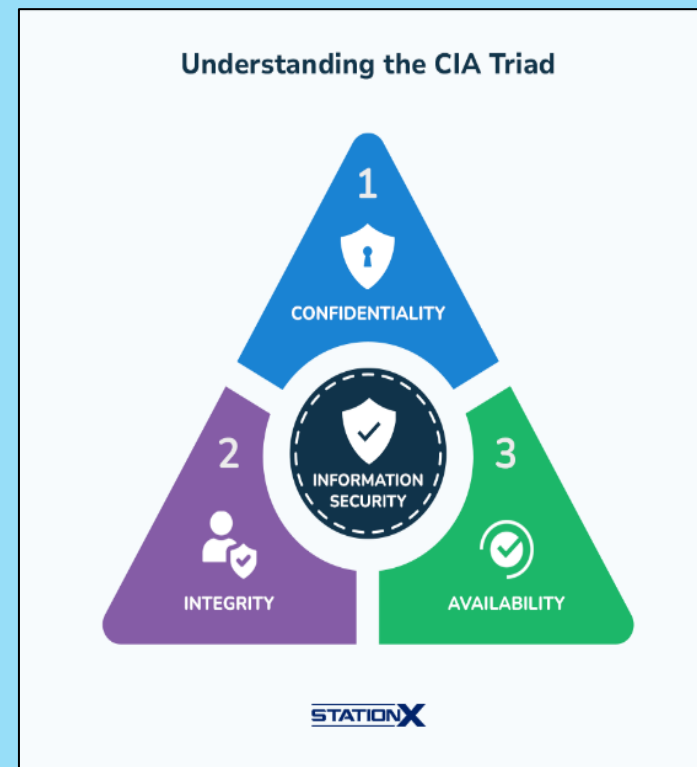
Objective 2: To assess the challenges and benefits of ISO 27001 implementation – Identify common challenges and benefits associated with ISO 27001 implementation.

Objective 3: To develop a bespoke application for managing an Information Security Management System (ISMS) – Implementing an application that supports organisations in maintaining their ISMS.

3. Literature Review

The literature review explored the impact ISO 27001 has on organisational cybersecurity, highlighting its structured approach through the CIA triad (Confidentiality, Integrity and Availability) (Figure 1). Compared to NIST CSF, ISO 27001 offers certification and global recognition making ISO 27001 ideal for organisations such as LSN Diffusion Ltd. Case Studies such as Imptek Chova Ecuador showed the benefits and challenges of ISO 27001 implementation. The benefits include secure data protection and certification to improve the company's reputation, and the challenges include time consumption and continuous evolving threats. The AUTOSYS case study demonstrated how an ISMS application could be developed to help maintain ISO 27001 within organisations. Overall, ISO 27001 significantly enhances organisational cybersecurity but does require ongoing commitment to remain effective against the continuous evolving threats.

Figure 1: CIA Triad



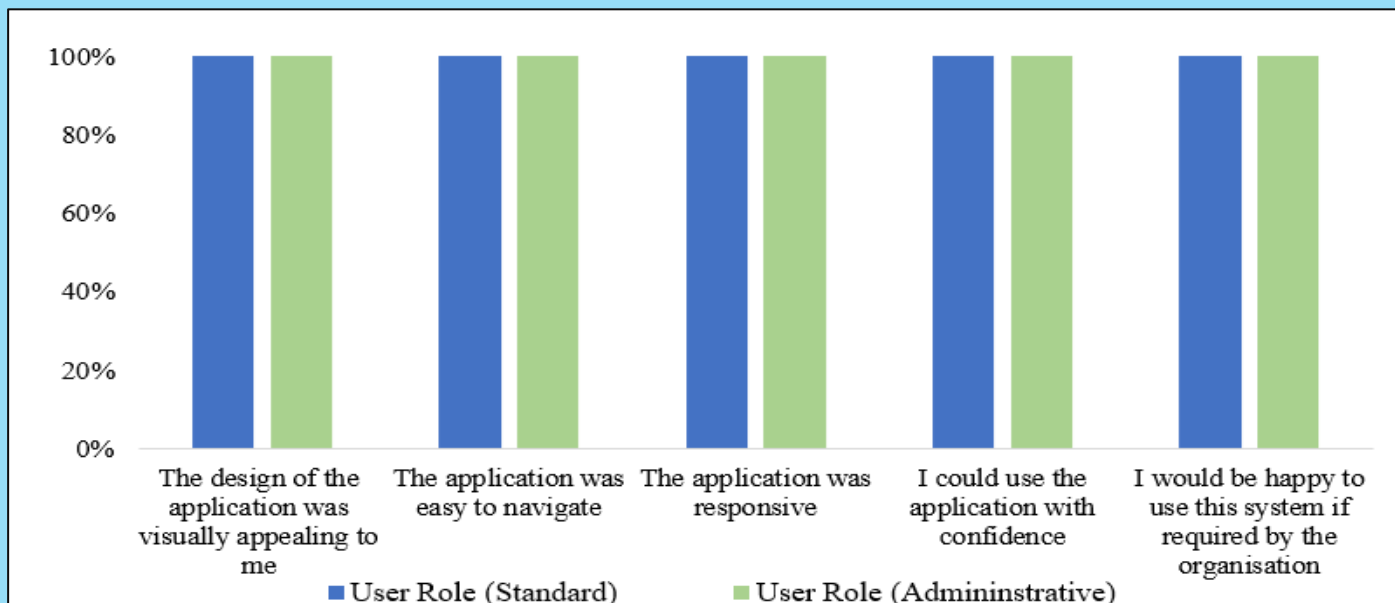
4. Method

- **Phase One (Pre-Development):** Interviews with key staff at LSN Diffusion Ltd.
- **Phase Two (Post-Development):** Usability testing to evaluate the applications performance and user experience.
- **Research Framework:** Guided by the Saunders Research Onion.
- **Data Collection Approach:** Mixed Methods combining qualitative interviews and quantitative surveys (usability testing) to collect data.
- **Development Tools Used:** Node.js, Express.js, PostgreSQL and Docker – used to build the bespoke ISMS application.

5. Implementation and Results

The ISMS application was developed to support LSN Diffusion Ltd to maintain their ISO 27001 certification. The application was designed to enable users to complete tasks such as submitting data security incident, change request and access request forms, policy management and a dashboard presenting data submitted into the application. Usability testing results of the developed ISMS application proved to be very positive. Both administrative and standard users reported high satisfaction with the performance and design of the application. Figure 2 illustrates a summary of the key results from participant feedback (scoring very well/well) following the usability testing phase of this project.

Figure 2: Usability Testing Results



6. Conclusion

The project evaluated ISO 27001's impact on cybersecurity and developed a custom ISMS application to support compliance. Findings confirmed ISO 27001's structured approach improves security with advantages over other frameworks such as NIST CSF. Case studies highlighted both benefits and challenges, while the AUTOSYS showed how an ISMS application can ease maintaining ISO 27001. The application addressed key challenges and performed well during usability tests.

7. Recommendations

Recommendations from this project include: enhance the ISMS application further by developing mobile access, form status tracking, risk assessments, and consider future opportunities for artificial intelligence (AI) integration. Future research opportunities include an impact assessment of ISO 27001 over a longer period of time, and further exploration of the standard's implementation and impact in other organisations