National College of Ireland

Enhancing Information Security Management System using ISO controls-based framework.

M.Sc. Industry Internship
M.Sc. In Cyber Security

Abhishek Shetty
Student ID: 21176078

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Abhishek Shetty
Student ID:	21176078
Programme:	Msc. In Cyber Security **Year:** 2022-23
Module:	Msc. Industry Internship
Supervisor:	Prof. Vikas Sahni
Submission Due Date:	04/09/2023
Project Title:	Enhancing Information Security Management System using ISO controls-based framework
Word Count:	6637 **Page Count**. 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Abhishek Shetty
Date:	01/09/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Information Security Management System using ISO controls-based framework

Abhishek Shetty
21176078

ABSTRACT

This research paper presents a comprehensive framework for achieving ISO 27001:2022 compliance and enhancing information security practices. The analysis begins with an exploration of the ISO 27001:2022 standard and its vital role in modern cybersecurity. It details a dynamic web-based framework, developed using React JS, that catalogues and explains all 93 controls specified by the standard. The framework aids organizations in conducting gap analyses and evaluating adherence to controls.
The research emphasizes the synergy of automated analysis through the framework and human assessment of internal policies. By manually assessing confidential documents, organizations gain a nuanced perspective on their security measures. The paper advocates for a holistic approach to addressing gaps, incorporating industry best practices. By bridging these gaps and implementing missing controls, organizations bolster their information security posture and proactively mitigate cyber threats. In essence, this research guides organizations in navigating complex information security landscapes while safeguarding critical assets.

Keywords*: Information security, Gap analysis, ISO 27001:2022, Controls implementation, web framework*

1 Introduction

In the rapidly evolving digital landscape, information security has emerged as a paramount concern for organizations worldwide. With the ever-increasing sophistication and frequency of cyber threats, safeguarding sensitive data and maintaining the integrity of information systems have become critical imperatives to ensure business continuity and uphold customer trust. Data Resolve Technologies, a leading technology firm, recognizes the significance of robust information security practices and has embarked on a comprehensive gap analysis to assess its current security measures against the international standard ISO 27001:2022. This research endeavours to delve into the findings of the gap analysis conducted at Data Resolve Technologies and proposes a model for implementing best practices to address the identified gaps effectively. By doing so, this study aims to provide Data Resolve Technologies with invaluable insights to bolster its information security posture and fortify its

defences against cyber threats. In recent years, the information security landscape has witnessed a significant transformation. Cyberattacks, once considered isolated events, have now evolved into sophisticated and widespread campaigns that target organizations of all sizes. The repercussions of such attacks can be catastrophic, leading to financial losses, reputational damage, and compromised customer data. As a result, organizations like Data Resolve Technologies are increasingly realizing the necessity of adopting proactive and resilient security measures. To demonstrate its commitment to information security best practices, Data Resolve Technologies has aligned me to perform gap analysis and build a security framework with the ISO 27001:2022 standard controls. Using the ISO 27001:2022 I am building a comprehensive framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). This standard is globally recognized and serves as a benchmark for organizations aiming to bolster their information security posture and adhere to best practices.

The primary objectives of the gap analysis conducted at Data Resolve Technologies were twofold. First, the analysis aimed to identify potential weaknesses and shortcomings in the existing information security policy structure. This is achieved by performing the manual gap analysis. By aligning with the ISO 27001:2022 standard, I am helping the organization to bridge the gaps and enhance its security measures. Second, the study aimed to prioritize the areas for improvement, allowing Data Resolve Technologies to allocate its resources efficiently and effectively. The methodology employed in this research encompassed various data collection techniques, including interviews, documentation reviews, and technical assessments. Key stakeholders, such as IT personnel, security experts, and management, actively participated in the gap analysis process. Their collaboration ensured a comprehensive evaluation of the existing information security practices. Through this research, several critical gaps, and vulnerabilities in Data Resolve Technologies' current information security measures were identified. The gaps spanned across organizational controls, people control, physical controls, and technological controls. Understanding these areas of weakness is crucial to developing an effective strategy for improvement. To address the identified gaps and bolster its information security posture, Data Resolve Technologies is embarking on the implementation of a tailored model. This proposed model emphasizes the integration of technical solutions, robust policies, and comprehensive employee training. By fostering a culture of cybersecurity awareness, the organization aims to instil a proactive and vigilant approach to information security among its workforce.

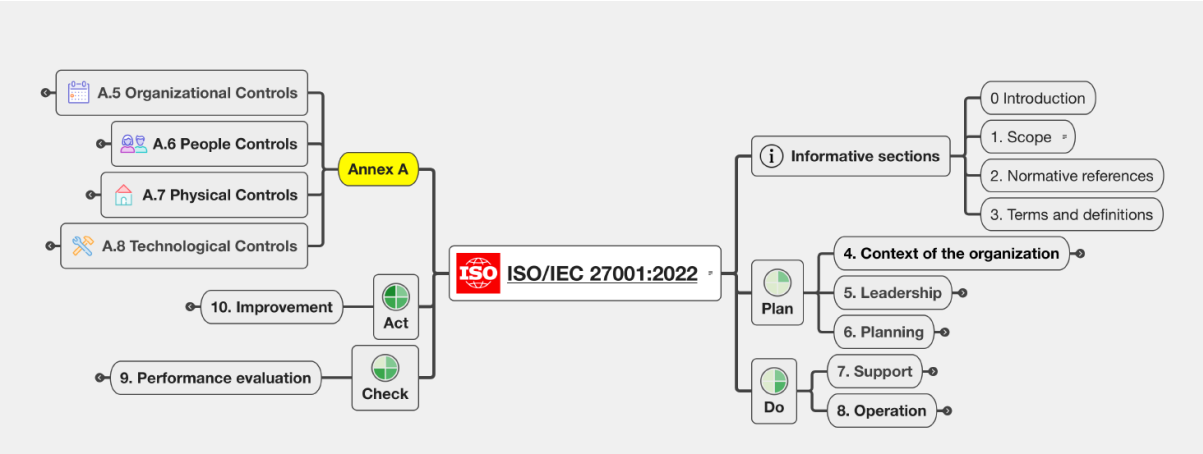

Fig 1: ISO/IEC 27001:2022 PDCA mindmap(Lange, 2022)

The above image is a figure made by Aron Lange, one of the famous Lead Implementors of the ISO 27001:2022. Taking a little guidance from the above model, this research undertaking serves as a vital steppingstone for Data Resolve Technologies to reinforce its information security practices. By aligning with the ISO 27001:2022 standard and adopting the proposed implementation model, the organization can establish a secure and resilient digital environment. In doing so, Data Resolve Technologies aims to enhance customer trust, safeguard its intellectual property, and position itself as a trusted leader in the competitive technology industry.

1.1 Research Question

How to enhance the company's infosec posture by addressing the identified gaps from the ISO 27001:2022 gap analysis using the Gap analysis web framework to mitigate cyber threats?

1.2 Research Objective

Fortify the company's information security system, minimize vulnerabilities, and establish a resilient defence against evolving cyber threats.

2 Related Work

2.1 Challenges and Approaches in Implementing ISO 27001:2022 ISMS

In (Ade Wahyu & Muhammad, 2023) their study titled "Recommendations for Designing Information Security Framework in Government Procurement of Goods/Services Certification Systems based on ISO 27001:2022," addresses security challenges in government procurement. They focus on enhancing information security through ISO 27001:2022-based controls. The researchers explore existing certification processes, highlight security gaps, and propose a comprehensive security framework categorized into organizational, people, physical, and technological controls. Their framework aims to bridge security gaps, strengthen integrity,

and ensure credible certification. The study underscores the importance of a robust security framework for government procurement, with potential implications for future enhancements in shared network environments.

This discussion by (Podrecca & Sartor, n.d.) presents the first analysis of ISO/IEC 27001, a crucial international standard for information security. The study employs Grey Models (GM) - including Even GM (1,1), Even GM (1,1,α,θ), Discrete GM (1,1), and Discrete GM (1,1,α) - alongside relative growth rate and doubling time indexes to analyse ISO/IEC 27001 adoption across six major countries. Findings reveal an anticipated growing trend in the standard's adoption, with China projected to lead globally. The research contributes to the field by introducing a forecasting approach uncommon in the realm of international standards. It addresses the limited diffusion of ISO/IEC 27001 despite its significance in ensuring information security. The paper's methodology and results offer insights into future adoption patterns, aiding companies, certification bodies like ISO, policymakers, and industries in aligning strategies, enhancing data protection, and understanding potential areas of improvement. Limitations include the need to consider external factors impacting adoption and potential expansion to study other management standards. The study encourages further investigation into ISO/IEC 27001's motivations, challenges, and effectiveness in diverse contexts.

The paper (Junaid, 2023) discusses ISO 27001, an essential framework for implementing Information Security Management Systems (ISMS) to protect information systematically and cost-effectively. ISO 27001 offers guidelines to establish, operate, and enhance ISMS. The paper details the ISO 27001 structure, its evolution, and its certification process. It emphasizes the importance of aligning security with safety requirements, exemplified by a cyberattack on a water treatment plant. The paper advocates following the Plan-Do-Check-Act (PDCA) cycle for ISMS implementation and highlights the interconnectedness of security and safety. By complying with ISO 27001, organizations can enhance their security posture and protect critical systems and data in an evolving digital landscape.

Here, (Legowo & Juhartoyo, 2022) the paper examines the risk assessment of an information technology security system at a bank using ISO 27001. It identifies security vulnerabilities in electronic banking services and conducts risk assessments based on ISO 27001's Annex A checklist. The study evaluates information technology security system maturity, finding 75% compliance on average, with business continuity management at 55% and domain compliance at 93%. Risk assessment reveals three assets with very high inherent risk and seven with high risk. The paper recommends implementing 19 control measures and emphasizes prioritizing high-risk assets. The study underscores the importance of aligning security and safety and suggests a cost-benefit analysis for control implementation.

In this article by (Kitsios et al., 2023) emphasizes the importance of data privacy, accessibility, and authenticity for enterprises, highlighting the need for robust security strategies to counter cyber threats. It outlines a plan implemented by an IT firm to comply with ISO 27001, assessing motivations and benefits. The study showcases a risk management framework within an international IT consulting services institution, aligning procedures with ISO 27001 guidelines. The challenges of maintaining security amidst rapid expansion and customer expectations are discussed. The paper underscores risk assessment's pivotal role in developing effective

information security strategies and acknowledges its ongoing nature. ISO 27001 implementation is presented as a dynamic process in response to evolving risks.

The article by (Erkaboev Abrorjon & Alikhonov Elmurod, 2022) discusses the integration of ISO 9001 and ISO/IEC 27001 standards, focusing on information security and quality management. It highlights the significance of safeguarding information amidst technological advancements. Both standards share a process approach, structure, and objectives, enabling synergistic integration. ISO 9001 emphasizes quality, customer satisfaction, and measurable goals, while ISO/IEC 27001 prioritizes information security, risk management, and business continuity. The integration of these systems is seen as crucial for modern businesses to excel by ensuring product/service quality and information security. The article underscores the growing interdependence of these aspects for market leadership.

This (Marhavilas et al., 2022) paper focuses on the development of a risk assessment framework for implementing an information security management system (ISMS) compliant with ISO 27001 in the information technology sector. It underscores the importance of safeguarding information against increasing cyber threats and explores the challenges of implementing an effective ISMS. The study examines a multinational IT consulting services company that deals with large business support projects. The paper discusses the risk assessment process, the management of necessary configurations, and the difficulties faced. The practical contributions include providing practitioners with a framework for ISMS implementation and optimization. However, the lengthy risk assessment process and the need for broader case studies are acknowledged as limitations.

The research by (Marhavilas et al., 2022) discusses the implementation of an Information Security Management System (ISMS) based on the ISO 27001 standard to protect information systems. It emphasizes the importance of ISMS in ensuring data confidentiality, integrity, and availability. The PDCA (Plan-Do-Check-Act) cycle is highlighted as a method for continuous improvement. The phases of planning, implementation, checking, and acting are explained, including risk analysis, security measures, and compliance audits. The article concludes that ISMS is crucial for organizations to enhance security, gain credibility, and foster development. ISO 27001 and ISO 27002 standards are referenced for guidance on ISMS implementation.

The (Malatji, 2023) paper compares ISO/IEC 27001:2022 and ISO/IEC 27001:2013 using the NIST Cybersecurity Framework (CF) lens, examining security controls. The ISO/IEC 27001:2022, a widely used standard for info security, was updated to address global cybersecurity challenges. The study finds both editions share similar security control distribution within NIST CF functions. Protect Function is emphasized. ISO/IEC 27001:2022 introduces 11 new controls, including cloud computing security, not explicit in NIST CF. The paper suggests potential improvements like addressing IoT security. Five key ISO/IEC 27001:2022 changes are detailed: minor Clauses 4-10 changes, 11 new controls in Annex A, decreased controls (114 to 93), grouped controls, and updated title focusing on global cybersecurity challenges and digital trust.

(Ramadhan & Rose, 2022) This research focuses on adapting the ISO/IEC 27001 Information Security Management Standard to Small and Medium Enterprises (SMEs). SMEs face challenges in selecting and implementing security standards effectively. ISO 27001's role and a framework for SMEs' ISO 27001 implementation are explored. The study emphasizes SMEs'

need to manage the Confidentiality, Integrity, and Availability (CIA) of information. The suggested framework includes steps like obtaining management support, defining scope, risk assessment, implementing controls, training, operating ISMS, management review, and monitoring. Challenges in implementation and benefits of ISO 27001 for SMEs are discussed. Future work could involve combining ISO 27001 with other standards and exploring similar adaptations in different contexts.

The article (Murphy, 2022)emphasizes that cybersecurity is no longer just an IT concern but a critical business aspect impacting insurance costs. Stakeholders demand detailed cybersecurity practices. ISO/IEC 27001 certification is a key assurance tool. Aligning internal controls with the NIST Cybersecurity Framework (CSF) and ISO 27001 is crucial. A mature Information Security Management System (ISMS) is necessary for ISO 27001. The ISO stages involve adopting a framework, risk assessment, controls mapping, and audit. Risk assessment involves impact and likelihood factors. The "do" stage includes control implementation and training, while the "check" and "act" stages focus on monitoring, improvement, and certification. Successful certification enhances confidence and reduces risks.

2.2 Industry research on InfoSec management system, physical security, risk assessment and Threat intelligence

The study by (Nordmark & Källebo Rebermark, 2023) examines perceptions of information security in a hybrid work context, focusing on a Swedish IT consultancy firm. It employs the Protection Motivation Theory (PMT) and ISO standards to analyze interviews with six employees. The findings reveal diverse views on information security while working remotely. The office environment significantly influences perceived security, with social interactions aiding education and awareness. Employee education is crucial, although ISO 27001:2022 is deemed insufficient for addressing remote work. The study highlights the multi-faceted nature of remote work security and the need for updated standards to align with evolving work models.

This research (Taherdoost, 2022b) explores the significance of cybersecurity standards in safeguarding valuable data from loss or theft. Cybersecurity involves protecting sensitive data from damage or theft, and various procedures and standards are crucial for its successful implementation. This research presents a narrative review of frequently used cybersecurity standards and frameworks, examining their applications across industries. By analyzing 17 papers published between 2000 and 2022, the study aids businesses in selecting the most appropriate cybersecurity standards and frameworks based on their specific requirements. The paper underscores the importance of standards in mitigating cyber threats, enhancing security, and facilitating compliance with industry best practices.

This study by (Taherdoost, 2022a) explores the role of different types of Management Information System (MIS) applications in business development. MIS plays a crucial role in gathering, analyzing, storing, and disseminating data for decision-making, control, and analysis. The paper discusses the fundamental activities of MIS - input, processing, output, and feedback - and how it supports various levels of an organization: operational, management, and strategic. It highlights six main types of MIS applications - Data Processing Systems, Process Control Systems, Enterprise Information Systems, Decision Support Systems, Executive Information Systems, and Management Information Systems. The study emphasizes the positive impact of MIS on business efficiency, growth, and productivity.

The study by (Sensuse et al., 2022) focuses on establishing an initial cybersecurity framework for Indonesia's new capital city, Ibu Kota Nusantara (IKN), which aims to be a smart, livable city with critical infrastructure. Using a systematic literature review, the study identifies factors

such as smart city, livable city, and critical infrastructure, and proposes security objectives including confidentiality, integrity, availability, safety, and privacy. The framework suggests employing technologies like big data, blockchain, biometrics, machine learning, cryptography, AI, and intrusion detection. Risk assessment, security governance, and awareness are also recommended. The study highlights the need to align IKN's development principles with cybersecurity goals, ensuring comprehensive protection through technology and strategies.

In the context of increasing digitalization, this paper (Agyepong et al., 2023) examines how companies assess and interpret their information security using metrics, particularly about ISO/IEC 27001:2022 standards. Despite the established normative standards, companies often fulfil requirements minimally and lack a comprehensive view of their security and risk impact. The study explores the relationship between decision-makers security interpretations, effectiveness, and conformity. Existing practices and frameworks for measuring and certifying information security systems are analyzed. The research highlights a need for a more holistic security perspective and proposes a structured approach to address these challenges. The paper underscores the importance of accurate measurement and visualization to facilitate informed decision-making in information security.

This paper (Tintin & Hidalgo, 2023) discusses the implementation of an Information Security Management System (ISMS) model based on ISO/IEC 27001:2013 for safeguarding public data, using the Property Registry of Pedro Moncayo Canton (PRPMC) in Ecuador as a case study. The study explores how the ISMS model, combined with national regulations, ensures the security of public data and prepares for potential risks. The PRPMC's implementation of the ISMS model led to significant improvements in data security, achieving a high standard of 81% security. Ethical hacking reports demonstrate the system's effectiveness in identifying and addressing vulnerabilities. The study underscores the importance of international standards and recommends a broader adoption of such measures for protecting citizens' personal information.

This study (Stewart, 2022) addresses information security breaches caused by human errors despite existing standards and frameworks. It introduces the Nine Five Circles (NFC) framework for the Information Security Management System (ISMS) based on ISO27001:2013. The NFC combines human and technological factors to enhance ISMS. The study uses exploratory surveys in fifty financial institutes and finds that human-technology interrelationships contribute to security incidents. The NFC principle improves performance monitoring and interconnections compared to standalone ISMS standards. The research emphasizes the need for comprehensive ISMS, especially in the financial sector, and highlights NFC's benefits, suggesting it could be an effective approach for managing data breaches and improving cybersecurity.

This study (Amaro et al., 2022) addresses the increasing frequency of cyber-attacks and proposes a methodological framework for cyber threat intelligence (CTI). The framework collects, organizes, filters, shares, and visualizes cyber threat data to mitigate attacks and vulnerabilities. It introduces an eight-step CTI model with timeline visualization and analytics. A Python-based tool is developed as a proof of concept, allowing threat data collection, filtering, and visualization. The study highlights challenges in CTI, the need for standardization, and the importance of sharing information for quick threat mitigation. Future work includes improving visualization, analysis, and methodologies for collecting and sharing structured and unstructured data. The framework aims to enhance CTI effectiveness and facilitate threat discovery and mitigation.

The paper proposes (Chandra et al., 2022) the Delta ISMS method to strengthen company-wide information security management systems (ISMS) through incident learning. It acknowledges the need for feedback and learning from incidents in ISMS and introduces detailed procedures for incident learning, including an incident database operation method and a communication method for double-loop learning. The proposed procedures are supervised by the Chief

Information Security Officer and aim to enhance ISMS's PDCA cycles. The study emphasizes the importance of regularizing informal knowledge and double-loop learning for effective incident mitigation. The conclusion highlights the framework's contribution to improving cybersecurity risk assessments based on cyber situational awareness and an application-assisted approach.

The paper by (Glavan et al., 2023) focuses on Multi-Access Edge Computing (MEC) and its security analysis. MEC is a key technology in 5G networks, offering benefits like low latency and improved user experience. The study categorizes MEC-specific features, vulnerabilities, threats, and security measures, aligning them with ISO/IEC 27001:2022 controls. It addresses cloud-native architecture, distributed nature, complex multi-party environments, edge locations, and APIs. The authors highlight the need for security standards convergence between telecommunications and IT sectors due to MEC's role in 5G. The paper contributes by providing a comprehensive threat analysis and security measures for MEC in the context of emerging 5G networks.

2.3 Research Niche

Author Name	Strength	Weakness
Ade Wahyu & Muhammad (2023)	Comprehensive security framework proposal for government procurement using ISO 27001:2022 controls.	Limited discussion on potential challenges in framework implementation.
Podrecca & Sartor (n.d.)	First analysis of ISO/IEC 27001, forecasting adoption patterns and potential areas of improvement.	Limited discussion on external factors influencing adoption trends.
Junaid (2023)	Detailed exploration of ISO 27001's role, structure, and benefits for enhancing security posture in organizations.	Could provide more practical examples of organizations benefiting from ISO 27001 implementation.
Legowo & Juhartoyo (2022)	In-depth risk assessment of an IT security system using ISO 27001's Annex A checklist, offering control recommendations.	Could elaborate on specific challenges faced during control implementation.
Kitsios et al. (2023)	Real-world implementation of ISO 27001 in an IT consulting services firm, emphasizing risk management and compliance.	More insights could be provided on how scalability and expansion challenges were addressed.
Erkaboev Abrorjon & Alikhonov (2022)	Insightful comparison of ISO 9001 and ISO/IEC 27001 integration, highlighting their interdependence for quality and security management.	Could delve deeper into potential complexities encountered during the integration process.
Marhavilas et al. (2022)	Practical risk assessment framework for ISMS implementation in the IT sector, offering practical implementation insights.	More case studies or industry examples could enhance the paper's applicability to different scenarios.
Murphy (2022)	Detailed comparison of ISO/IEC 27001:2022 and ISO/IEC 27001:2013 using NIST CSF, highlighting key changes and their implications.	Could provide a more extensive analysis of the implications of IoT security in the new controls.

Ramadhan & Rose (2022)	Detailed framework for adapting ISO 27001 to SMEs, addressing the unique challenges faced by smaller organizations.	More practical examples of SMEs successfully adopting ISO 27001 could add depth to the paper.
Nordmark & Källebo Rebermark (2023)	A unique exploration of perceptions on information security in a hybrid work context, offering insights into the influence of the office environment.	Could discuss potential strategies to bridge ISO 27001's limitations for remote work security.
Taherdoost (2022b)	A comprehensive narrative review of cybersecurity standards and frameworks, assisting businesses in selecting appropriate ones.	This could include more discussions on the practical implementation challenges of different standards.
Taherdoost (2022a)	A thorough exploration of the role and types of Management Information Systems (MIS) in business development.	Could provide more industry-specific examples to illustrate MIS applications.
Sensuse et al. (2022)	Robust cybersecurity framework proposal for a new smart city, addressing the security needs of critical infrastructure.	Could provide more details on the integration of recommended technologies in the city's development.
Agyepong et al. (2023)	An insightful exploration of decision makers' security interpretations, effectiveness, and conformity, proposing a structured approach.	Could elaborate on the potential implications of a more holistic security perspective for businesses.
Tintin & Hidalgo (2023)	In-depth case study on ISMS model implementation for data security, showcasing significant improvements in protecting public data.	Could provide more insights into the challenges faced during the implementation process.
Stewart (2022)	Introduction of the NFC framework for ISMS based on ISO27001:2013, addressing the human-technology interrelationships in security.	This could include more discussions on the potential limitations of the NFC framework.
Amaro et al. (2022)	A comprehensive methodology for cyber threat intelligence (CTI) framework, offering a structured approach for threat discovery and mitigation.	Could elaborate on how the proposed framework addresses the challenge of sharing structured and unstructured data.
Chandra et al. (2022)	Detailed Delta ISMS method proposal for incident learning, enhancing incident mitigation, and cyber situational awareness.	Could discuss potential challenges and limitations in implementing the proposed procedures.
Glavan et al. (2023)	In-depth analysis of Multi-Access Edge Computing (MEC) security aligned with ISO 27001:2022 controls.	Could elaborate on how the suggested security measures are practically implemented in MEC environments.

3 Research Methodology

This section shows details of the method used in the gap analysis model. This section explains the procedure used for the ISO gap analysis framework. The purpose was to understand, build, and test the gap analysis framework using the controls given by the ISO27001:2022 for Data Resolve Technologies based in India, which is a cyber security-based company. This framework is built based on the Annex A controls. There are in total 93 controls that contribute

to getting the ISO27001:2022 certification. With the help of these controls, the company can understand the missing factors in the company's Information security management system. By implementing the framework, we can understand the controls that are missing and can plan and act upon to add the same.

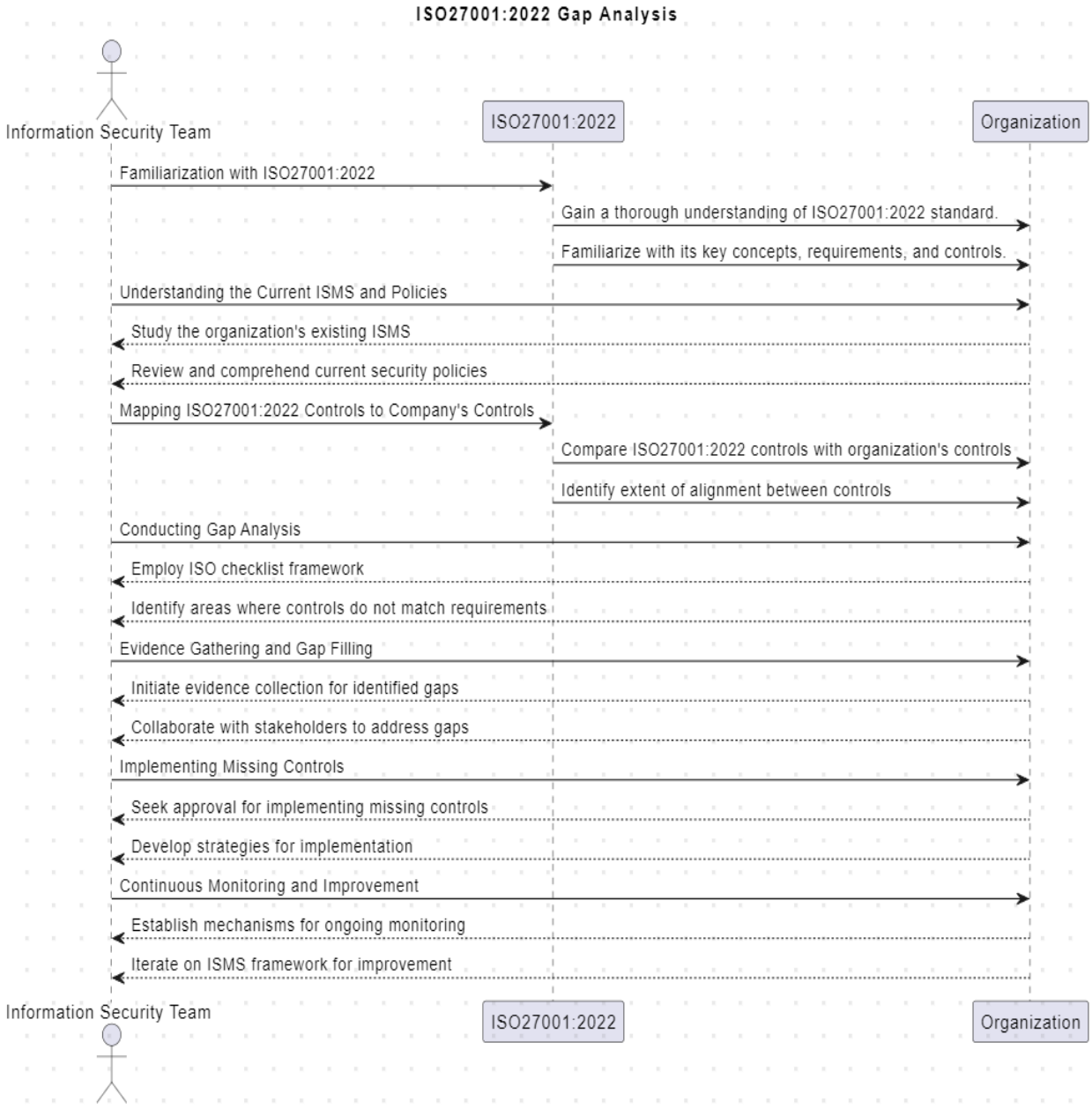

Fig 2: Sequence diagram of the ISO gap analysis

This sequence diagram illustrates the interaction between the Information Security Team, that is me as the Lead implementor of the ISO controls, and the Organization during the gap analysis of ISO27001:2022. Each stage is represented as a message exchange between the actors and participants involved. The diagram shows the flow of activities, from familiarization with the standard to continuous monitoring and improvement of the ISMS framework. The stages are explained in more detail:

- **Stage 1**: Familiarized with ISO27001:2022: I gained a thorough understanding of the ISO27001:2022 standard, encompassing its fundamental principles, requirements, and controls. This involved studying its comprehensive framework for information security management.
- **Stage 2**: Understood the Current ISMS and Policies: I immersed myself in studying the organization's existing Information Security Management System (ISMS), delving into its structure, components, and operational intricacies. This enabled me to comprehend the current security protocols, policies, and associated documents that the company follows.
- **Stage 3**: Mapped ISO27001:2022 Controls to Company's Controls: I meticulously compared the controls outlined in ISO27001:2022 with the organization's established security controls. This thorough examination facilitated the identification of overlaps, deviations, and gaps between the two sets of controls.
- **Stage 4**: Conducted Gap Analysis: Utilizing the ISO checklist framework, I performed a comprehensive gap analysis, systematically assessing the extent to which the organization's existing controls aligned with the requirements specified by ISO27001:2022. This critical step revealed areas where our controls fell short.
- **Stage 5**: Gathering Evidence and Filling Gaps: I initiated the process of collecting evidence to support the identified gaps. Collaborating closely with relevant stakeholders, strategies were developed to address these gaps systematically.
- **Stage 6**: Implementing Missing Controls: Upon obtaining approval from organizational management, strategies were formulated to implement the necessary controls, aligning them with ISO27001:2022 requirements. This ensured a structured approach to enhancing our information security framework.
- **Stage 7**: Continuously Monitoring and Improving: Mechanisms were established for ongoing monitoring of the implemented controls. Lessons learned from the gap analysis will be used to refine the Information Security Management System (ISMS) framework, fostering continuous enhancement and alignment with ISO27001:2022 standards.

4 Design Specification

Following a thorough familiarization with the ISO27001:2022 controls and a comprehensive understanding of the Information Security Management System (ISMS) implemented within the company, in conjunction with the review of all established security policies, the subsequent phase involved the meticulous process of correlating these controls with the existing framework encompassed by the organization's ISMS and the associated security policies. This precise assessment constituted a pivotal component of the overall strategy, systematically assessing the congruence between the established organizational security protocols and the rigorous standards mandated by ISO. As a result of this detailed examination, a comprehensive list featuring all 93 controls as delineated in the ISO27001:2022 update was compiled, serving as a foundational reference for subsequent gap analysis and enhancement efforts. This exhaustive analysis yielded invaluable insights into the organization's current information security infrastructure and paved the way for targeted improvements aligned with international standards. Below is the representation of all the 93 controls present in the ISO27001:2022 update:

5 Organizational controls (37)	6 People Controls (8)
5.1 Policies for information security	6.1 Screening
5.2 Information security roles and responsibilities	6.2 Terms and conditions of employment
5.3 Segregation of duties	6.3 Information security awareness, education and training
5.4 Management responsibilities	6.4 Disciplinary process
5.5 Contact with authorities	6.5 Responsibilities after termination or change of employment
5.6 Contact with special interest groups	6.6 Confidentiality or non-disclosure agreements
5.7 Threat intelligence	6.7 Remote working
5.8 Information security in project management	6.8 Information security event reporting
5.9 Inventory of information and other associated assets	
5.10 Acceptable use of information and other associated assets	
5.11 Return of assets	
5.12 Classification of information	
5.13 Labelling of information	
5.14 Information transfer	
5.15 Access control	
5.16 Identity management	
5.17 Authentication information	
518 Access rights	
5.19 Information security in supplier relationships	
5.20 Addressing information security within supplier agreements	
5.21 Managing information security in the ICT supply chain	
5.22 Monitoring, review and change management of supplier services	
5.23 Information security for use of cloud services	
5.24 Information security incident management planning and preparation	
5.25 Assessment and decision on information security events	
5.26 Response to information security incidents	
5.27 Learning from information security incidents	
5.28 Collection of evidence	
5.29 Information security during disruption	
5.30 ICT readiness for business continuity	
5.31 Legal, statutory, regulatory and contractual requirements	
5.32 Intellectual property rights	
5.33 Protection of records	
5.34 Privacy and protection of PII	
5.35 Independent review of information security	
5.36 Compliance with policies, rules and standards for information security	
5.37 Documented operating procedures	

7 Physical controls (14)	8 Technological Controls (34)
7.1 Physical security perimeters	8.1 User endpoint devices
7.2 Physical entry	8.2 Privileged access rights
7.3 Securing offices, rooms and facilities	8.3 Information access restriction
7.4 Physical security monitoring	8.4 Access to source code
7.5 Protecting against physical and environmental threats	8.5 Secure authentication
7.6 Working in secure areas	8.6 Capacity management
7.7 Clear desk and clear screen	8.7 Protection against matware
7.8 Equipment siting and protection	8.8 Management of technical vulnerabilities
7.9 Security of assets off-premises	8.9 Configuration management
7.10 Storage media	8.10 Information deletion
7.11 Supporting utilities	8.11 Data masking
7.12 Cabling security	8.12 Data leakage prevention
7.13 Equipment maintenance	8.13 Information backup
7.14 Secure disposal or re-use of equipment	8.14 Redundancy of information processing faclities
	8.15 Logging
	8.16 Monitoring activities
	8.17 Clock synchronization
	8.18 Use of privileged utility programs
	8.19 Installation of software on operational systems
	8.20 Networks security
	8 21 Security of network services
	8.22 Segregation of networks
	8.23 Web filtering
	8.24 Use of cryptography
	8.25 Secure development lifecycle
	8.26 Application security requirements
	8.27 Secure system architecture arid engineering principles
	8.28 Secure coding
	829 Security testing in development and acceptance
	8.30 Outsourced development
	8.31 Separation of development, test and production environments
	8.32 Change management
	8.33 Test information
	8.34 Protection of information systems during audit testing

Table 1: ISO controls

1

[1] What are the 11 new security controls in ISO 27001:2022? (advisera.com)

As we can see in the above Tables 1 and 2 are lists of controls categorized under four types: Organizational, People, Physical, and Technological controls. Each control here will be picked up and will be compared with the organization's ISMS and security documentation. A manual mapping was conducted first with the process to identify the list of missing controls. The manual task was tedious and time-consuming, and hence a web-based framework was developed. This framework was built using React JS and is hosted on Git Hub.

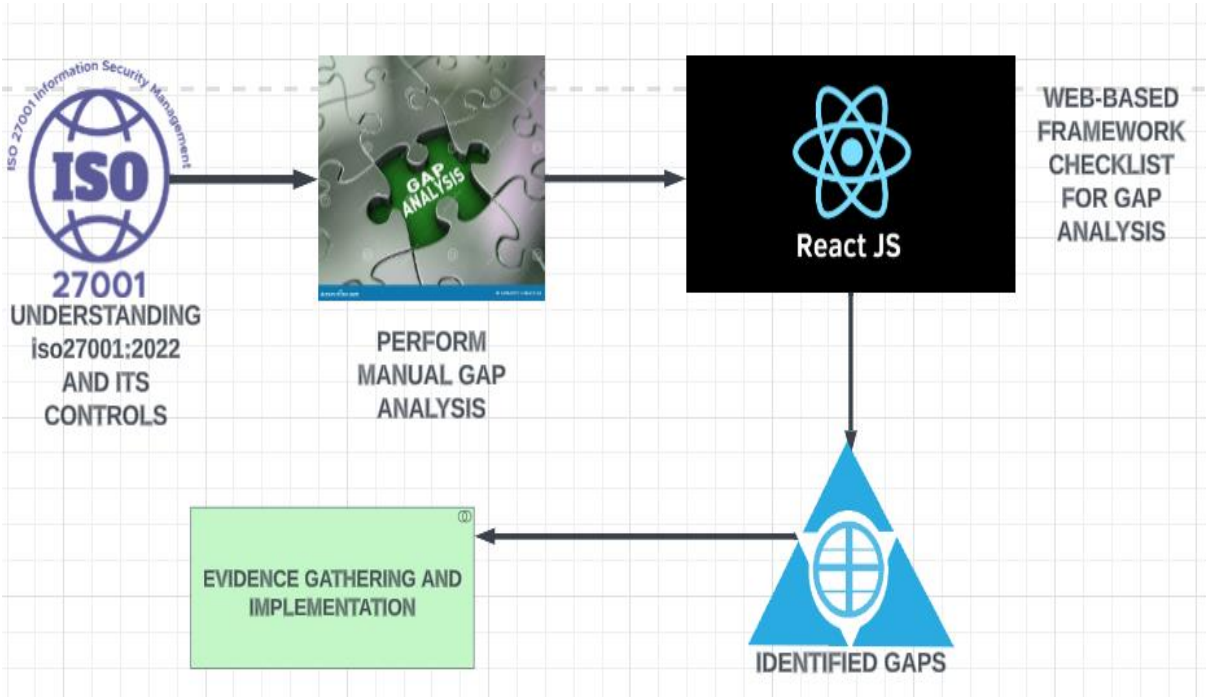

Fig 3: Workflow of the gap analysis

Fig 3 represents the flow of gap analysis that was conducted for this organization. First, there was an analysis and understanding of ISO27001:2022. Following that, manual tasks were performed, which were tedious and took days together. To save time, the organization decided to speed up the process and thus there was the implementation of a webpage to perform the gap analysis using the react JS code that gave a framework with a list of controls and a checklist that shows the steps if the control is missing and what can be done to implement the missing controls.

5 Implementation

The implementation phase of the project is based on building a web-based framework using React JS to conduct a comprehensive gap analysis based on ISO27001:2022 controls. This innovative approach aimed to streamline the gap analysis process, overcome the limitations of manual mapping, and provide a user-friendly platform for evaluating the organization's Information Security Management System (ISMS) against international standards.

Control Number	Control Description	Present in IT Security Policy	Gap Explanation
5.5	Contact with authorities	No	The policy does not provide guidelines for contact with authorities in security incidents.
5.6	Contact with special interest groups	No	The policy does not address contact with special interest groups concerning security matters.
5.7	Threat intelligence	No	The policy does not include guidelines for gathering and utilizing threat intelligence.
5.19	Information security in supplier relationships	No	The policy does not cover information security aspects in supplier relationships.
5.2	Addressing information security within supplier agreements	No	The policy does not include guidelines for addressing security in supplier agreements.
5.21	Managing information security in the ICT supply chain	No	The policy does not address managing security in the ICT supply chain.
5.22	Monitoring, review, and change management of supplier services	No	The policy does not provide guidelines for monitoring and reviewing supplier services.
5.23	Information security for use of cloud services	No	The policy does not include guidelines for securing the use of cloud services.
5.24	Information security incident management planning and preparation	No	The policy does not cover incident management planning and preparation.
5.25	Assessment and decision on information security events	No	The policy does not provide procedures for assessing and deciding on security events.
5.26	Response to information security incidents	No	The policy does not address the response process for information security incidents.
5.27	Learning from information security incidents	No	The policy does not include processes for learning from security incidents.
5.28	Collection of evidence	No	The policy does not provide guidelines for the collection of evidence related to incidents.
5.29	Information security during disruption	No	The policy does not address information security during business disruptions.
5.3	ICT readiness for business continuity	No	The policy does not include guidelines for ICT readiness during business continuity incidents.
5.35	Independent review of information security	No	The policy does not specify the requirement for an independent review of information security, which helps ensure an impartial assessment of security measures.
6.1	Screening	No	The policy does not provide specific guidelines and procedures for screening employees, etc.
6.2	Terms and conditions of employment	No	The policy does not address information security requirements in employment terms and conditions.
6.4	Disciplinary process	No	The policy does not detail the disciplinary process for security policy violations.
6.5	Responsibilities after termination or change of employment	No	The policy lacks clear procedures for managing information security upon termination or change.
6.6	Confidentiality or non-disclosure agreements	No	The policy does not address confidentiality agreements to protect sensitive information.
6.8	Information security event reporting	No	The policy does not provide guidelines for reporting information security events.
7.1	Physical security perimeters	No	The policy does not cover physical security perimeters for facilities.
7.2	Physical entry	No	The policy lacks specific controls for managing physical entry to secure areas.
7.3	Securing offices, rooms, and facilities	No	The policy does not provide measures for securing offices and rooms within the organization.
7.4	Physical security monitoring	No	The policy does not address monitoring physical security aspects.
7.5	Protecting against physical and environmental threats	No	The policy does not include guidelines for protecting against physical and environmental threats.
7.6	Working in secure areas	No	The policy does not provide guidelines for working in secure areas.
7.8	Equipment siting and protection	No	The policy does not address equipment siting and protection measures.
7.9	Security of assets off-premises	No	The policy does not cover the security of assets when off-premises.
7.1	Storage media	No	The policy does not include guidelines for secure storage media usage.
7.11	Supporting utilities	No	The policy does not address the security of supporting utilities.
7.12	Cabling security	No	The policy does not include guidelines for cabling security.
7.13	Equipment maintenance	No	The policy does not provide measures for equipment maintenance related to security.
7.14	Secure disposal or re-use of equipment	No	The policy does not cover secure disposal or re-use of equipment.

Table 2: Manual gap analysis

In the above table, as you see the manual gap analysis was conducted for individual controls, and the ones that are missing are updated in the framework assessment, Recognizing the complexity and time-consuming nature of manual gap analysis, the decision was made to leverage technology to enhance the process. React JS, a popular JavaScript library for building user interfaces was chosen for its flexibility, interactivity, and ease of development. The framework was designed to function as an interactive webpage, combining a structured list of controls from ISO27001:2022 with an efficient checklist to evaluate control adherence. The framework was developed with a user-centered design approach. The user interface was designed to be intuitive, easy to navigate,

and visually appealing. Controls were categorized into organizational, people, physical, and technological groups to enhance user comprehension and engagement. Each control was accompanied by a brief explanation to aid users in understanding its significance.

The workflow of the web-based gap analysis was carefully planned to mirror the manual analysis process while leveraging the advantages of automation. Users started by selecting a control from the categorized list. The framework then provided a checklist, guiding users through a series of questions and criteria to assess control adherence within the organization. For controls identified as missing or not fully adhered to, the framework offered a comprehensive checklist outlining the steps required for implementation. This proactive approach transformed the gap analysis from a mere assessment into a strategic tool for improving information security. Each checklist item was tailored to the specific control, enabling users to understand the scope of necessary actions and fostering a clear roadmap for implementation.

Fig 4: ISO27001:2022 control checklist web framework

The above figure is a snapshot of the web-based control framework. The introduction of the web-based framework significantly improved the efficiency of the gap analysis process. Instead of manually cross-referencing controls and documentation, users could swiftly navigate through the controls, access explanations, and make assessments within a user-friendly environment. This not only saved valuable time but also minimized the risk of human error that can occur during manual evaluations.

One of the key advantages of the web-based framework was its capacity to facilitate collaboration among stakeholders. Different individuals and teams within the organization responsible for various controls could access the framework, contribute assessments, and discuss implementation steps. This collaborative feature ensured that a holistic understanding of controls' status and requirements was achieved, fostering a collective effort towards compliance.

6 Evaluation

The evaluation section of the project work shows the major findings of the research as well as the analysis results giving an illustration of both manual and web-based evaluation results

6.1 Case Study I: Results of the manual gap analysis

In the context of enhancing information security measures, a manual gap analysis was undertaken for Data Resolve Technologies to bridge the divide between its existing Information Security Management System (ISMS) and the internationally recognized ISO27001:2022 standards. This case study delves into the process and outcomes of this meticulous examination.

The initial phase involved a comprehensive understanding of the ISO27001:2022 standard, with a focus on its controls, requirements, and best practices. This laid the foundation for a structured analysis that followed. By immersing myself in Data Resolve Technologies' ISMS, security policies, and associated documents, I gained insights into the company's existing security landscape. This familiarity provided a solid platform for the subsequent mapping and assessment of controls.

Undertaking the manual gap analysis required meticulous attention to detail. Each control outlined in the ISO27001:2022 was scrutinized against Data Resolve Technologies' current controls. This entailed a systematic comparison to identify areas of convergence and divergence. Through this meticulous process, the project highlighted where the organization's security measures aligned seamlessly with ISO standards and, conversely, where gaps existed.

The web page is a brief representation of some of the controls that produce the results in Table 3

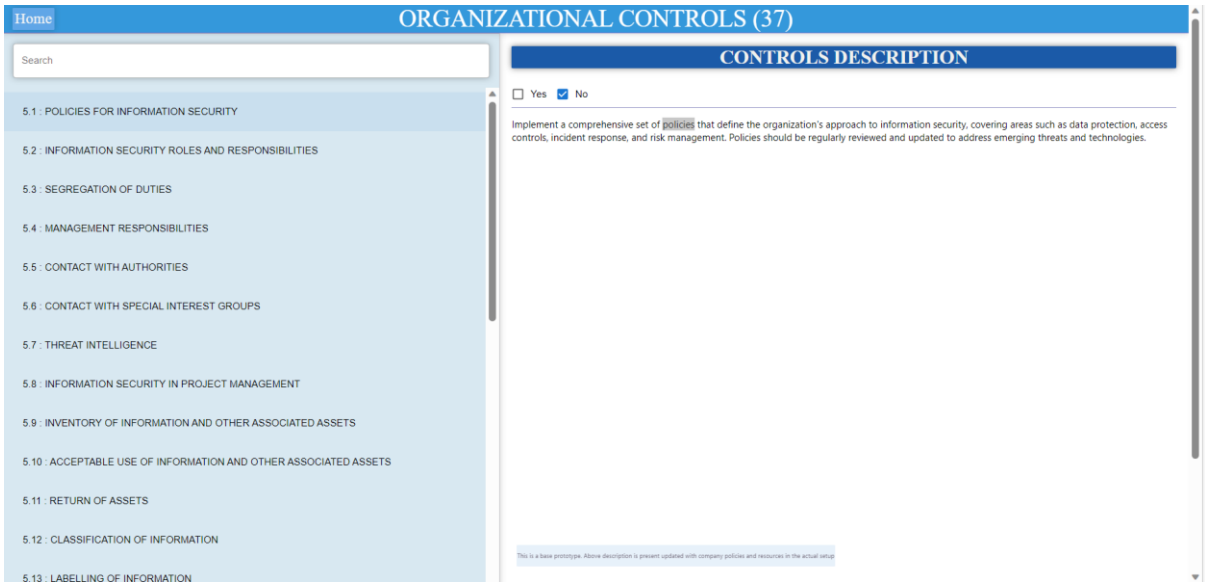

Fig 5: Web checklist framework of ISO 27001:2022 gap analysis

Control Number	Control Description	Objectives and Expected Outcomes	Resources Allocation	Implementation Plan	Documentation and Training	Technical Implementation	Monitoring and Review	Incident Response and Management	Communication and Reporting	Continuous Improvement
5.5	Contact with authorities	Establish a clear process for interacting with relevant authorities in case of security incidents or regulatory requirements.	IT Security Team, Legal Team	Develop guidelines for engaging with authorities and define roles and responsibilities.	Conduct training sessions for IT and relevant staff on how to handle interactions with authorities.	Implement a designated point of contact for authorities and establish communication protocols.	Regularly review and update the contact list and communication procedures.	Define incident response procedures for reporting security incidents to authorities.	Communicate incident reporting procedures to all employees and relevant stakeholders.	Periodically review and update the contact list and procedures based on feedback and changes in regulations.
5.6	Contact with special interest groups	Establish guidelines for interactions with special interest groups to ensure that sensitive information is not disclosed and organizational interests are protected.	Communications Team, Legal Team	Develop a policy for engaging with special interest groups and define authorized spokespersons.	Provide training to relevant staff on the policy and guidelines for interacting with special interest groups.	Implement secure communication channels and methods for engaging with special interest groups.	Regularly review and assess interactions with special interest groups to ensure compliance with established guidelines.	Develop procedures for addressing incidents or breaches related to interactions with special interest groups.	Document and report interactions with special interest groups, ensuring that sensitive information is not disclosed.	Analyze the effectiveness of the guidelines and procedures for interactions with special interest groups and make improvements as needed.
5.7	Threat intelligence	Establish processes for gathering and utilizing threat intelligence to proactively identify and mitigate potential security threats.	IT Security Team, Threat Intelligence Providers	Develop procedures for collecting, analyzing, and disseminating threat intelligence.	Provide training to the IT Security Team on the use of threat intelligence tools and resources.	Implement threat intelligence feeds and platforms to receive and analyze real-time threat data.	Regularly review threat intelligence reports and assess their relevance to the organization's security posture.	Develop incident response procedures based on threat intelligence to address emerging threats.	Share relevant threat intelligence information with relevant stakeholders and partners.	Evaluate the effectiveness of the threat intelligence processes in identifying and mitigating threats and make adjustments as needed.
5.19	Information security in supplier relationships	Establish clear information security requirements for suppliers to ensure the security of shared data and systems.	Procurement Team, IT Security Team	Develop information security requirements and guidelines for suppliers and vendors.	Provide training to procurement staff on incorporating security requirements into supplier agreements.	Include information security clauses in supplier agreements, specifying security controls, responsibilities, and reporting obligations.	Periodically assess supplier compliance with information security requirements through audits and assessments.	Define incident response procedures for addressing security breaches or failures by suppliers.	Establish a reporting mechanism for suppliers to communicate security incidents or breaches to the organization.	Review and analyze supplier agreements and relationships to identify areas for improvement in information security requirements.

Table 3: Evaluation of Gap Analysis Framework

The manual nature of this analysis brought to light its challenges, particularly in terms of time consumption and the potential for human error. However, it also enabled a deep dive into the organization's specific context and security practices. This approach proved instrumental in identifying nuanced gaps that might not have been as evident through automated means.
The case study also highlighted the necessity for streamlining this process. To address this, a web-based gap analysis framework using React JS was designed. This tool expedited the identification of missing controls by automating much of the comparative work. The framework served as a robust repository of controls, their descriptions, and the required steps for implementation.
The manual gap analysis for Data Resolve Technologies exemplified the value of detailed, contextual exploration. It uncovered specific gaps in their information security framework and paved the way for more targeted enhancements. This experience further underscored the significance of technological solutions, like the web-based framework, to simplify and expedite the process, ultimately fortifying the organization's information security posture in a dynamic digital landscape.

7 Conclusion and Future Work

7.1 Conclusion

The successful implementation of the web-based ISO27001:2022 gap analysis framework represents a pivotal milestone in the organization's pursuit of robust information security practices. By harnessing the synergy between cutting-edge technology and internationally recognized standards, the project has substantially elevated the efficiency and effectiveness of the gap analysis process. This implementation is not merely a technological achievement; it symbolizes a strategic commitment to fostering a culture of information security excellence. The framework's ability to seamlessly integrate complex control evaluations into a user-friendly interface has streamlined an otherwise intricate task. This has empowered stakeholders at all levels to actively contribute to the organization's information security landscape. The project's success underscores the immense potential of automation to revolutionize traditional practices in the realm of information security. It establishes a precedent for future endeavours, inspiring further exploration of how technology-driven solutions can be harnessed to address critical security challenges.
As the organization continues its journey towards information security excellence, the future enhancements of the framework will play a pivotal role in further refining its functionality and adaptability. By remaining responsive to evolving needs and leveraging technology's ever-expanding capabilities, the organization ensures its continued alignment with global best practices and its resilience against emerging security threats.

7.2 Future Works

While the implemented web-based ISO27001:2022 gap analysis framework has already demonstrated its efficacy, its evolution remains an ongoing process with possibilities for continuous enhancement. The inherent flexibility of technology-driven solutions opens the door to several avenues for refining the framework's capabilities, making it an even more indispensable tool for the organization's information security journey.

Advanced Reporting Functionality: An immediate enhancement could involve the integration of advanced reporting functionalities. These functionalities would allow the framework to generate comprehensive and detailed gap analysis reports. Such reports could

provide stakeholders with a clear and structured overview of the organization's control adherence status, highlighting areas of strength and potential vulnerabilities. These reports would be invaluable for decision-makers, auditors, and compliance officers seeking a holistic view of the organization's information security posture.

Real-Time Collaboration Features: To further enhance communication and teamwork among various stakeholders, the framework could be enriched with real-time collaboration features. Features such as comment sections, discussion threads, or collaborative workspaces would foster open dialogue among team members responsible for control implementation. This real-time interaction could facilitate the exchange of ideas, insights, and progress updates, creating a dynamic environment conducive to effective collaboration and problem-solving.

Automated Reminders and Notifications: Another enhancement could involve the incorporation of automated reminder and notification functionalities. The framework could be programmed to send automated reminders to stakeholders regarding pending tasks, deadlines, or milestones related to control implementation. This would not only serve as a useful organizational tool but also ensure that control implementation stays on track, minimizing the risk of delays and oversights.

8. References

Ade Wahyu, K., & Muhammad, S. (2023). *View of Recommendations for designing information security framework in government procurement of goods/services certification systems based on ISO 27001:2022*.

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2023). A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers and Security*, *124*. https://doi.org/10.1016/J.COSE.2022.102959

Amaro, L. J. B., Azevedo, B. W. P., de Mendonca, F. L. L., Giozza, W. F., Albuquerque, R. de O., & Villalba, L. J. G. (2022). Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data. *Applied Sciences 2022, Vol. 12, Page 1205*, *12*(3), 1205. https://doi.org/10.3390/APP12031205

Chandra, N. A., Ramli, K., Ratna, A. A. P., & Gunawan, T. S. (2022). Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. *Risks 2022, Vol. 10, Page 165*, *10*(8), 165. https://doi.org/10.3390/RISKS10080165

Erkaboev Abrorjon, K. ogli, & Alikhonov Elmurod, J. (2022, September). *View of About the Integration of Information Security and Quality Management*. https://geniusjournals.org/index.php/erb/article/view/2157/1878

Glavan, A. F., Gheorghica, D., & Croitoru, V. (2023). MULTI-ACCESS EDGE COMPUTING ANALYSIS OF RISKS AND SECURITY MEASURES. *REVUE ROUMAINE DES SCIENCES TECHNIQUES — SÉRIE ÉLECTROTECHNIQUE ET ÉNERGÉTIQUE*, *68*(2), 206–211. https://doi.org/10.59277/RRST-EE.2023.68.2.15

Junaid, T.-S. (2023). *ISO 27001: Information Security Management Systems Real-Time Facial Detection and Recognition with Minimum Tagged Data Through a Distributed Publish Subscribe Network View project Real-time Smart Attendance System Using Facial Recognition for Working from Home and Video Conference. View project ISO 27001: Information Security Management Systems*. https://doi.org/10.13140/RG.2.2.36267.52005

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability 2023, Vol. 15, Page 5828*, *15*(7), 5828. https://doi.org/10.3390/SU15075828

Lange, A. (2022). *ISO27001 Lead Implementor*. https://www.google.com/imgres?imgurl=https://i.ytimg.com/vi/jvhWqp4Cx8M/maxresdefault.jpg&tbnid=Eh6M00daIi_6uM&vet=1&imgrefurl=https://tn.linkedin.com/posts/aronlange_connecting-the-dots-mapping-the-relationships-activity-7042797448410357760-h7de&docid=rdM9qsKFgi_R0M&w=1280&h=720&itg=1&source=sh/x/im/m5/1

Legowo, N., & Juhartoyo, Y. (2022). Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. *Online) Journal of System and Management Sciences*, *12*(3), 181–199. https://doi.org/10.33168/JSMS.2022.0310

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference on Cyber Management and Engineering, CyMaEn 2023*, 117–122. https://doi.org/10.1109/CYMAEN57228.2023.10051114

Marhavilas, K., Boustras, G., Koulouriotis, D. E., Tajani, F., Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability 2022, Vol. 14, Page 1269*, *14*(3), 1269. https://doi.org/10.3390/SU14031269

Murphy, G. (2022, July). *THE JOURNEY TO ISO 27001 CERTIFICATION - ProQuest*. https://www.proquest.com/docview/2679855443?fromopenview=true&pq-origsite=gscholar

Nordmark, J., & Källebo Rebermark, O. (2023). *Information security and hybrid work : A case study of shifts in perceived information security when working hybridly*. https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-505397

Podrecca, M., & Sartor, M. (n.d.). *Forecasting the diffusion of ISO/IEC 27001: a Grey model approach*. https://doi.org/10.1108/TQM-07-2022-0220

Ramadhan, N., & Rose, U. (2022). *Adapting ISO/ IEC 27001 Information Security Management Standard to SMEs*.

Sensuse, D. I., Putro, P. A. W., Rachmawati, R., & Sunindyo, W. D. (2022). Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology. *Information 2022, Vol. 13, Page 580*, *13*(12), 580. https://doi.org/10.3390/INFO13120580

Stewart, H. (2022). Why do ISO27001 Certified Organizations Still Experience Data Leakage? Design and Evaluation of Cyber-attack Prevention Strategies covering Technological and Human Aspects View project. *Article in Journal of Digital Information Management*, *20*. https://doi.org/10.6025/jdim/2022/20/3/90-103

Taherdoost, H. (2022a). *The Role of Different Types of Management Information System Applications in Business Development: Concepts, and Limitations*. https://papers.ssrn.com/abstract=4285861

Taherdoost, H. (2022b). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics 2022, Vol. 11, Page 2181*, *11*(14), 2181. https://doi.org/10.3390/ELECTRONICS11142181

Tintin, R., & Hidalgo, M. (2023). Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Protect Public Data? *2023 9th International Conference on Democracy and EGovernment, ICEDEG 2023*. https://doi.org/10.1109/ICEDEG58167.2023.10122109