*Majors: MIS*
*Major/No. MIS 3*

# *"Implementing Smart Compliance by Experimenting with Predictive Documentation and Intelligent ISO 27001 Checklist in AI-Driven Governance"*


**By:**

***(Ali Afzal)*** ***(01-321242-004)***

**Supervisor:**
**(Zahra Saleem)**

**HR and Management Department**

**Bahria Business school**
**Bahria University Islamabad**

**Fall 2026**

# FINAL PROJECT/THESIS APPROVAL SHEET

## Open Defense Examination

Open Defense Date __/__/____

**Topic of Research:** (***Implementing Smart Compliance by Experimenting with Predictive Documentation and Intelligent ISO 27001 Checklist in AI-Driven Governance***)

**Names of Student(s):** Ali Afzal Enrol # *01-321242-004*

- 
- 
- 

**Class:** (MBA/1.5/MIS)

**Approved by:**

_____

**(Zahra Saleem)**

Supervisor

_____

**Qurat Ul Ain Waqar**

Research Coordinator

_____

**Dr. Aftab Haider**

Head of Department

## ACKNOWLEDGEMENT

From the deepest of my heart, I would like to thank Almighty Allah for the unconditional love and strength He has shown me throughout my life, enabling me to cope with every challenge that came my way. I would like to sincerely thank and appreciate the efforts of my supervisor, Ms. Zahra Saleem, whose dedicated commitment, professional guidance, encouraging attitude, and unwavering support made the completion of this dissertation possible within the limited time available. I am extremely grateful to my family for their constant love and support through every phase of my life, as they have been the primary reason behind my success and achievements in my master's degree. I owe a great debt of gratitude to my parents for their continuous support and for being a constant source of motivation throughout my life. I would also like to appreciate the support of my graduate friends, who helped me greatly throughout my graduate studies.

## ABSTRACT

Information security has become a critical concern for organizations worldwide, and ISO/IEC 27001:2022 provides a recognized framework for managing information security risks, improving governance, and enhancing stakeholder trust. Despite these benefits, many organizations delay or avoid implementing the standard due to high costs, complex documentation, limited internal expertise, and time constraints. This study investigates the challenges in ISO/IEC 27001 implementation and evaluates the role of a smart, AI-driven predictive ToolKit, which consists of semi-automated documentation and an intelligent ISO 27001 checklist, in supporting effective, efficient, and sustainable compliance.

A quantitative research approach was adopted using a cross-sectional survey design. Data were collected from information security professionals and analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) in SmartPLS 4. The study examined the relationships between perceived benefits of ISO/IEC 27001, implementation difficulty, organizational avoidance behavior, and the effectiveness of the AI-enabled predictive ToolKit.

The findings reveal that while organizations recognize the strategic and operational benefits of ISO/IEC 27001, perceived implementation difficulty remains a major barrier, leading to avoidance behavior. The results further show that the AI-driven predictive ToolKit reduces this difficulty by simplifying documentation, providing clear guidance, and offering a dynamic, intelligent ISO 27001 checklist to monitor compliance. Implementation difficulty and ToolKit effectiveness were found to mediate the relationship between perceived benefits and actual adoption of ISO/IEC 27001.

Overall, this research demonstrates that AI-enabled predictive ToolKits, integrating documentation and intelligent checklists, can transform ISO/IEC 27001 implementation from a complex, manual process into a guided, manageable, and sustainable practice. The study provides practical recommendations for organizations, practitioners, and ToolKit developers, contributing to both academic knowledge and real-world governance, risk, and compliance practices.

# Contents

# Chapter 1: Introduction

## 1.1. Background of study

In the modern digitalized world, information has emerged as one of the most valuable assets in organizations in all industries (Böhme & Moore, 2021). Companies are increasingly relying on the digital technologies, cloud computing, remote work environments and intertwined information systems to facilitate their day to day operations, strategic decision making and service provision (Smith & Tan, 2020). These technologies enhance effectiveness, scalability and innovativeness, however, they present serious dangers to information security (Verma et al., 2019).

A broad spectrum of threats has been revealed to businesses today such as cyberattacks, ransomware, phishing, insider threats, data breach, unauthorized access and regulatory non-compliance (ENISA, 2021). Cyber attacks may interfere with operations, incur losses, reputation tarnishment, and penalties, as well as customer mistrust. Consequently, information security has ceased to be a technical matter and is now strategic and governance, which has to be managed in a structured manner and constantly monitored (ISO/IEC, 2022a).

Organizations implement formal Information Security Management Systems (ISMS) in order to overcome such challenges. The ISO/IEC 27001:2022 is a global standard that gives an organized guideline on the management of information security risks (ISO/IEC, 2022b). It outlines provisions on how to set up, operationalize, sustain and continually enhance an ISMS. The standard focuses on risk-based approach in that the choice of security controls is based on organizational context, value of assets, and risk exposure as opposed to applying general or non-essential security controls (ISO/IEC, 2022b).

The most recent update of ISO/IEC 27001 of 2022 contained some useful modifications to introduce clarity, usability, and responsiveness to the modern organizational environment. Such updates will include changes in the control structure, the more focused leadership engagement, the organizational environment, and compliance with other management system standards such as such as ISO 9001:2015 (Quality Management) and ISO/IEC 20000-1:2018 (IT Service Management) (ISO, 2015; ISO/IEC, 2018). However, despite all these developments, more and more organizations are attempting to understand and implement the standard in practice.

One of the most urgent issues of the organizations is the complexity of the ISO/IEC 27001 documentation requirements. The standard requires much documentation including policies, procedures, risk assessment and risk treatment plans, asset inventories, applicability and evidences of continuous improvement (ISO/IEC, 2022b). Such documentation needs can overburden the organization with little internal knowledge especially the small and medium-sized enterprises (SMEs).

Manually, organizations are traditionally relying on external consultants to help gain the compliance to ISO/IEC 27001. Paperwork methods are slow, inconsistent and subject to human error. Excess use of consultants can lead to having generic documentation that might meet the audit requirement but it would not be representative to the actual processes, risks, and culture of the organization. Moreover, such dependence restricts internal learning and limits the potential of the organization to retain and enhance the ISMS on its own in the long term (Von Solms & Von Solms, 2020).

However, as the progress of artificial intelligence (AI), automation and decision-support technologies is gaining rapid momentum, there is an increasing opportunity to enhance the manner in which organizations are pursuing ISO/IEC 27001 compliance. Smart tools can offer formalized guidance, automate tedious documentation process, decrease mistakes, and assist organizations to comprehend intricate requirements to a better degree. Nevertheless, the introduction of these tools to ISO/IEC 27001 documentation is mediate in the research and practice.

Intelligent checklists may be also facilitated by the AI-driven governance tools which can be adjusted to the size of the organizations, industry, maturity level, and risk exposure. Available tools have the potential to forecast documentation holes, suggest applicable controls, and minimize human error based on the past inputs and patterns of compliance (Rahman et al., 2022). Nevertheless, the increasing use of AI in cybersecurity and governance has not been associated with much in the documentation and compliance support of ISO/IEC 27001, and the application of AI in the standard continues to have limited academic coverage and practice.

This study focuses on these issues by suggesting the creation of an intelligent, AI-assisted, semi-automated documentation ToolKit and intelligent ISO/IEC 27001 checklist. The suggested ToolKit will provide a stepwise way of leading the organization through the documentation and compliance process with organization-specific prompts instead of generic templates. The toolkit will save time, money, and manpower and enhance accuracy, consistency, and internal engagement (Gløersen, 2024).

The ToolKit promotes learning, information security practice ownership and sustainability by promoting internal teams instead of replacing them. It is anticipated that organizations that apply the ToolKit will have reduced reliance on external consultants, build greater business strengths and that compliance with ISO/IEC 27001 is perceived as an ongoing management initiative and not an exercise in certification (Gløersen, 2024).

The present study is based on the article by Borgny Louise Gløersen (2024), which is called Developing a Cyber Security Documentation Package to Project Deliveries. That research has emphasized the challenges in which organizations meet the cybersecurity requirements and provide consistent written documentation, especially when operating on a project-based environment within the oil and gas industry. Although the study was able to prove the importance

of documented structures in documentation, its industry-based scope restricts its relevance to other industries.

In order to address this drawback, the present study suggests the reusable, flexible, and AI-assisted documentation ToolKit in line with ISO/IEC 27001:2022. The proposed ToolKit, on the contrary, will be applicable to organizations of various sectors, sizes, and maturity levels, unlike the industry-specific solutions. This increased wider applicability enhances the applicability and contribution of the study.

## 1.2. Problem Statement

One of the most important standards for information security management is ISO/IEC 27001 (ISO/IEC, 2022a). However, many businesses find it difficult to establish and uphold compliance, particularly small and medium-sized businesses. Complex and extensive documentation requirements, a lack of internal expertise, a heavy reliance on outside consultants, and the time and expense of manual compliance tasks are the primary obstacles. Because of this, ISO 27001 implementation is frequently viewed as difficult and onerous, which results in avoidance, partial adoption, or superficial compliance.

Although ISO 27001 has obvious advantages like improved risk management, stronger governance, and increased stakeholder trust, these benefits are frequently insufficient to overcome implementation challenges. There is very little use of intelligent or automated tools for documentation and decision-making in current compliance procedures, which are primarily manual and consultant driven. Furthermore, AI-based or predictive documentation solutions that could improve internal process ownership and streamline compliance have received little attention in academic research.

This gap points out the need to find out if an AI-assisted predictive documentation toolkit can minimize organizational avoidance, lower perceived implementation difficulty, and promote more successful and long-lasting ISO/IEC 27001 compliance.

## 1.3. Research Questions & Hypotheses

This paper examines the issues that have already been established. It tries to resolve the following critical questions:

**Research Question 1:**

What are the main benefits of following ISO/IEC 27001 standards?

**Research Question 2:**

What difficulties do organizations commonly face during ISO/IEC 27001 implementation?

**Research Question 3:**

Why do some organizations still avoid ISO/IEC 27001 certification despite its benefits?

**Research Question 4:**

What is the impact of the application of an AI-supported, smart, semi-automated documentation ToolKit and intelligent checklist on the ISO/IEC 27001: 2022 compliance in your organization?

The hypotheses that will help the study to address the research question and prove the efficiency of the suggested ToolKit and ISO/IEC 27001 compliance practices are the following:

**Direct Effect Hypotheses**

**H1:** Implementation Difficulty has a positive relationship with ISO/IEC 27001.

**H2:** The Organizational Avoidance Reasons have a positive correlation with Implementation Difficulty.

**H3:** The positively correlated benefits of ISO/IEC 27001 are linked with the perceived effectiveness of the ToolKit.

**H4:** ToolKit Effect has a negative correlation with Organizational Avoidance Reasons.

**Hypotheses of Mediating Effect.**

**H5:** There is a relationship between Benefits and Avoidance Reasons which is mediated by Implementation Difficulty.

**H6:** ToolKit Effect is an intervening variable between Benefits and Avoidance Reasons.

## 1.4. Research Objectives

The primary objective of the research is to examine issues affecting the compliance of ISO/IEC 27001:2022 in organizations and introduce a smart, semi-automated, AI-based documentation ToolKit, which can be used to assist in achieving compliance effectively and correctly. In a bid to attain this objective, the study is aimed at accomplishing the following objectives:

**Research Objective 1:**

To investigate the effect of perceived Benefits of ISO/IEC 27001 on the Implementation Difficulty.

**Research Objective 2:**

To examine the effects of Implementation Difficulty on the Organizational Avoidance Reasons.

**Research Objective 3:**

To explore whether Benefits and Avoidance Reasons relate to Implementation Difficulty.

**Research Objective 4:**

To evaluate how Benefits influence the perceived effectiveness of the ToolKit.

**Research Objective 5:**

To examine whether the ToolKit reduces Organizational Avoidance Reasons.

**Research Objective 6:**

To evaluate the mediation of ToolKit Effect between the Benefits and Reasons to avoid.

## 1.5. Significance of Study

The research would be important as it tackles both scholarly and industry practical problems regarding the implementation of the ISO/IEC 27001:2022. The suggested AI-assisted ToolKit is beneficial to organizations, practitioners, and researchers because it yields to more efficient documentation, makes it cost-effective, and enhances the internal engagement.

### 1.5.1. Practical Value for Organizations

The study gives an intelligent, semi-automated ToolKit that makes documentation simple, saves time and is easy to use, and assists the organization to manage compliance more effectively. This is applicable to small organizations that have limited resources as well as large organizations that deal with intricate security demands.

### 1.5.2. Reduced Dependence on External Consultants

Consultants are critical in most organizations because of the lack of expertise. The proposed ToolKit is user-friendly and provides automated assistance that allows organizations to develop enhanced internal capacity and lower compliance expenses in the long run.

### 1.5.3. Improved Accuracy and Consistency

Hand written documentation is typical of errors. The intelligent ToolKit will allow the use of standardized, correct, and consistent documentation in line with ISO/IEC 27001:2022, which minimizes the risk of errors in audits.

### 1.5.4. Enhanced Internal Engagement

The compliance is simplified and made more comprehensible by the study, which encourages active involvement by the internal teams. This enhances the awareness, responsibility and ownership of information security practices.

### 1.5.5. Academic Contribution

The study addresses the gaps in the existing research because it proposes reusable, flexible and smart methodology of ISO/IEC 27001 compliance, which has not been thoroughly investigated in

earlier studies. It broadens the scholarly knowledge about the use of automation and smart tools to aid information security management systems.

### 1.5.6. Contribution to Industry Practices

The ToolKit offers an effective, modern and affordable strategy that can be embraced by organizations in the various fields. It helps enhance better preparedness to cyber threats and enhances the culture of security and compliance.

## 1.6. Scheme of the Study

This thesis is organized in five chapters, which aim to answer particular issues of the research problem and at the same time accomplish the objectives of the study. The chapters are well structured logically in order to give clarity and coherence and systematic way of presenting the research.

Chapter 1: Introduction

The chapter addresses the background of the research and identifies the increasing significance of the information security and ISO/IEC 27001:2022 compliance. It outlines research gap, states the problem and outlines research questions and hypotheses. Research objectives, the importance of the study and general layout of the thesis are also described in the chapter.

Chapter 2: Literature Review

In this chapter, the authors have monitored the literature available in the field of academia and industry regarding the implementation of ISO/IEC 27001, information security management system, documentation issues, organizational avoidance behavior, and the impact of automation and artificial intelligence in compliance. The review assists in laying the theoretical background of the research and aids in the formulation of the research model and hypotheses.

Chapter 3: Research Methodology.

This chapter describes the research design and methodological approach that was used in the study. It outlines the process of data collection, research tool (questionnaire), population to be studied, data gathering methodology and data analysis tools. The chapter also rationale the adopted methodology to give reliability and validity of the researched findings.

Chapter 4: Findings and Analysis of Data.

In this chapter, the analysis of collected data and discussion of the empiric findings are provided. It tests the hypotheses offered with the help of the relevant statistical methods and analyzes the connections between the most important variables including benefits, implementation difficulty, avoidance reasons, and the effectiveness of the suggested ToolKit. The findings give some of the

insights into the difficulties of implementing ISO/IEC 27001 and the role that an AI-assisted documentation ToolKit might play.

Chapter 5: Proposed ToolKit and Conclusion.

The last chapter presents the suggested intelligent ISO/IEC 27001 checklist and semi-automatic documentation ToolKit. It describes how the ToolKit can overcome the mentioned challenges and help to achieve successful compliance. The chapter also ends the study by summarizing the major findings, giving practical recommendations, discussing the limitations of the research, and giving suggestions on future research.

# Chapter 2: Literature Review

This chapter is designed to critically assess the available scholarly literature, the international standards, and even previous theses-level studies associated with the information security management and ISO/IEC 27001 application. The review provides the present study with a solid theoretical/practical base and helps the researcher to develop the very proposed research model and hypotheses proposed in Chapter 1.

The literature review considers the international information standards of security, the ISO/IEC 27001: 2022 including the information security control and governance standards like ISO/IEC 27002, which are used as a guideline on the information security controls and governance practices (ISO/IEC, 2022a; ISO/IEC, 2022b). These are the international standards of Information Security Management Systems (ISMS) and are extensively used in scholarly literature and in the field of practice. The discussion of these standards serves to clarify the purposes of these standards, requirements, and practical challenges, especially documentation and compliance.

Along with international standards, this chapter is reviewed with respect to earlier academic papers, journal articles, and Master and PhD theses that explore the benefits of ISO/IEC 27001, challenges of implementation, the organizational resistance, and the compliance behavior. Previous thesis research studies contribute useful empirical evidence on the implementation challenges experienced in the real world, particularly in the aspect of documentation work load, resource limitation, and reliance on outside consultants (Wanyonyi, 2019; Gløersen, 2024).

The chapter further examines the available studies on automation, smart systems and artificial intelligence (AI) in governance, risk and compliance (GRC). Although the automation and AI have been implemented widerly in compliance and cybersecurity, they are scarcely used in ISO/IEC 27001 documentation and checklist-based compliance assistance (ISO/IEC, 2023). This lapse is reflected in the literature of the subject and also in thesis work.

This chapter uses synthesis of the results of international standards, academic literature, and other associated theses to find the key themes, limitations, and gaps in the research. Such gaps are the reasons why an AI-based, semi-automated, documentation ToolKit and intelligent ISO/IEC 27001;2022 checklist should be proposed to simplify the implementation process, enhance the interest of the internal audience, and ensure the maintenance of compliance.

## 2.1. ISO/IEC 27001 and Information Security Management

The ISO/IEC 27001 is a globally accepted standard, which outlines the requirements in setting up, practice, sustaining and constant enhancement of an Information Security Management System (ISMS) (ISO/IEC, 2022a). The standard assumes a risk-based methodology to ensure the confidentiality, integrity and availability of information assets. The ISO/IEC 27001 is relevant to

organizations regardless of their sizes or fields and is aimed at making information security relevant to business goals.

The new standard ISO/IEC 27001:2022 made some structural and control modifications to enhance flexibility, clarity, and compatibility with other management systems standards of ISO. It gives more emphasis on organization setting, leadership engagement, risk management, and lean improvement. Even with these improvements, it is reported that organizations still experience problems in deciphering needs, drawing up documentation and ensuring compliance in the long term.

The ISO/IEC 27002 is a complement to the ISO/IEC 27001, as it has elaborate information security control guidelines. However, ISO/IEC 27002 is explanatory on how the controls may be implemented, but it lacks practical sections or automation mechanisms of documentation and monitoring compliance. Consequently, implementation of control is still to be interpreted and documented through manual means in organizations (ISO/IEC, 2022b).

## 2.2. Benefits of ISO/IEC 27001 Implementation

According to research, there are always several positive aspects of the use of ISO/IEC 27001, as it has led to better control of information security, minimized cyber risks, increased compliance with regulatory standards, and more trust in the organization (Wanyonyi, 2019; Gløersen, 2024). Certification also enhances the reputation of an organization and gives it competitive edge both in local and international markets.

Wanyonyi (2019) discovered that companies that deploy ISO/IEC 27001 are supported by the enhancement of internal processes, clearer risk management methods, and closer security-focused to business-related objectives. In the same manner, Glloersen (2024) pointed out that well-organized documentation of cybersecurity enhances transparency and responsibility in the setting.

There are however some studies that also suggest that the benefits however well known are not necessarily immediately adopted. Several organizations have recognized the importance of ISO/IEC 27001 and fear the perceived work and complexity of implementation (Wanyonyi, 2019).

## 2.3. Implementation Difficulty and Documentation Challenges

One of the most often mentioned impediments to the adoption of ISO/IEC 27001 is implementation difficulty. The standard involves a lot of documentation, which consists of policies, procedures, assessment of risk, assets inventories, statement of applicability, and demonstration of continual improvement (ISO/IEC, 2022a).

Studies indicate that manual documentation is very time consuming, ineffective, and subject to human error. Glloersen (2024) has noted that the engineers and the operational staff find it hard to

interpret the requirements of the cybersecurity and compliance, thus leading to incomplete or vague documentation.

Wanyonyi (2019) also emphasized that SMEs have difficulties associated with the lack of internal skills and financial resources. These complications make it more dependent on the use of consultants and add to the total cost of compliance, which strengthens the notion that ISO/IEC 27001 is complicated and challenging to upkeep.

## 2.4. Organizational Avoidance of ISO/IEC 27001

Organizational avoidance is the making of a choice not to get ISO/IEC 27001 certified or put it off even after being informed of its advantages. Major reasons of avoidance named in literature include the cost of implementation is very high, documentation is very complex, skilled resources are not available, management does not provide any support, and the return on investment is expected to be low.

Wanyonyi (2019) has observed that a lot of SMEs consider ISO / IEC 27001 to be a resource-consuming and challenging standard to maintain without an external support. Gløersen (2024) also established that the lack of clear documentation roles is one of the factors in the development of resistance and avoidance behavior.

These results verify the supposition that avoidance behavior is determined by more than benefits alone but also perceived difficulty and the presence of helpful instruments.

## 2.5. Role of Risk Management Standards

In ISO/IEC 27001 implementation, risk management is one of its essential parts. The standard is much related to the ISO 31000:2018 that offers the framework of identifying, analyzing, evaluating, and treating risks in an organized way (ISO, 2018).

The ISO 31000 highlights that management of risk ought to be well documented, involve stakeholders and be monitored. It has been documented in literature that poor or old documentation lowers the efficacy of risk assessment and creates ineffectual choice of control.

Risk registers in manual form do not keep up with evolving threat environments, which further supports the logic of structured and semi-automated documentation which this paper aims to achieve through structuring risk management in accordance with ISO/IEC 27001.

## 2.6. Automation and AI in Governance, Risk, and Compliance

Governance, risk, and compliance (GRC) activities are also being automated and subjected to artificial intelligence to improve their operations. Predictive analysis systems can cut human error, enhance consistency, and assist decision-making by AI-driven systems.

The ISO/IEC 42001:2023 provides a framework of a management system in artificial intelligence with a focus on responsible artificial intelligence practices, risk management, and management of the lifecycle. The standard aids the application of AI in organized and regulated organizational settings.

Despite the common use of AI in cybersecurity monitoring and threat detection, it is still not that common in terms of its application in ISO/IEC 27001 documentation and compliance support. This is a gap that points to the necessity of AI-based documentation ToolKit that offer intelligent direction and predictive compliance aid.

## 2.7. Review of Related Theses and Research

### 2.7.1. Cybersecurity Documentation Frameworks

An example of such a master thesis is Borgny Louise Gluedersen (2024), who wrote a thesis titled Developing a Cyber Security Documentation Package of Project Deliveries. The thesis was oriented on the issue of the difficulties encountered by suppliers operating in the oil and gas industry in response to the requirements of cybersecurity documentation created by various customers. The author noted that cybersecurity specifications are commonly applicable to the installation as a whole, whereas the suppliers only carry out a minimal part of the project. This discrepancy leads to confusion and complexity of the documentation.

The thesis also emphasized the fact that engineers working on supplier side do not always have enough knowledge of cybersecurity to have a clear vision of their duties. Based on the qualitative case approach using cases, it was found that there were gaps in the internal documentation practices and no standardized guidance was in the organization. As a solution to these challenges, the thesis developed a personalized system of cybersecurity documentation to cover the project deliveries of the suppliers.

The suggested model aligned recurrent cybersecurity specifications of various client specifications and mapped them to pertinent standards. Employee remarks showed that the framework enhanced the use, comprehension and knowledge of cybersecurity obligations at the project level. The applicability of the thesis to organizations in other sectors was, however, restricted by the fact that it was limited to a limited area to one industry and project based environments.

In spite of this drawback, the thesis powerfully proves the role of the systematic documentation systems and user-oriented tools. The results of the research are a direct contribution to the motivation of the current study, which further elaborates on this idea by suggesting a smart, reusable, and semi-automated documentation ToolKit that can be inherent to ISO/IEC 27001:2022 and applicable in various organizational settings.

### 2.7.2. Information Security ToolKit for ISO/IEC 27001

A thesis conducted by Victor Wekesa Wanyonyi (2019) was called Information Security Management ToolKit on ISO/IEC 27001 Standard: Case of Small-to-Medium Sized Enterprises

(SMEs). The thesis under analysis deals with the problem of SMEs in their efforts to implement ISO /IEC 27001 based on their limited resources, unawareness, and technical knowledge deficit.

The study came up with an information security management ToolKit which has been used to carry out the implementation of ISO/IEC 27001 controls in an organization. The ToolKit helped in risk identification, implementation of control measures and monitoring of progress. The results of the thesis revealed that SMEs were highly accepting of the ToolKit and appreciated the significance of the tool in streamlining the compliance process.

The thesis was able to conclude that the adoption of ToolKit can significantly decrease the barriers to the adoption of ISO/IEC 27001 with the help of affordable and structured ToolKit. Nonetheless, in the study, the emphasis was put more on the previous versions of the standard, and the intelligent or semi-automated documentation possibilities were not fully addressed. This fact shows that the development of Toolkit should be improved through additional research to increase its functionality and address the ISO/IEC 27001:2022 standards.

## 2.8. Research Gaps

Although ISO/IEC 27001:2022 is well-known as a necessary standard in information security management, the current studies point to a range of gaps in practice and the method of compliance:

Industry-Specific Focus: First, the existing studies are often industry- or organization-specific, i.e. oil and gas, healthcare, or financial services. Although these studies give useful information, the results are not always applicable to other sectors where risks are different and have other operational structures.

Little Practical Tools: Second, it is not having practical reusable tools, which help in the documentation of ISO/IEC 27001 in an organization specific way. Most solutions presently in the market are based on fixed templates, which do not go with the needs of organizations in terms of size, context and maturity. This typically results in documentation becoming a compliance exercise, and not a risk management exercise.

High Dependence on External Consultants: Third, the high dependence on external consultants is still a significant issue. Although consultants are involved to offer expertise, over-reliance adds to the expenses and the development of internal capability. The existing studies are not adequately concerned about the ways to decrease this dependency with the help of intelligent tools.

Manual and Error-Prone Processes: Traditional compliance processes: Traditional compliance processes imply manual documentation, which is time-consuming and inefficient and can be subjected to errors.

Small Internal Involvement: Existing methods typically do not engage internal organization participation and therefore, compliance is not considered as a risk management process, but a procedural one.

Lack of Predictive/Intelligent Support: Limited research exists on the use of intelligent semi-automated tools to direct organizations in complying with ISO/IEC 27001 in the proactive manner.

The proposed study fills these gaps by proposing a semi-automated, AI-assisted, and smart documentation ToolKit that improves usability, minimizes consultant dependency, helps to improve the quality of documentation, and encourages internal engagement.

## 2.9. Theoretical Support

The associated research is informed by the existing theory and principles of information security management, risk management, and compliance with the support of technology. The very concept of the ISO/IEC 27001 is rooted in the theory according to which the information security is to be handled in a systematic approach to the systematic improvement cycle that goes by the Plan-Do-Check-Act (PDCA) model. This model focuses on planning security controls according to risk, deploying it in practice, performance monitoring, and obtaining continuous improvement of the Information Security Management System (ISMS).

The theory of risk management also offers good theoretical support to this research. The ISO/IEC 27001 is similar to the ISO 31000 that focuses on the identification, analysis, evaluation and treatment of the risks in a systematic way. It has been demonstrated in the literature that proper risk management requires proper and consistent documentation which is current. Poor documentation lowers the effectiveness of risk evaluation and selection of risk control exposing security.

Moreover, the study is also backed with the theories of organizational learning and internal capability formation. Research indicates that excessive dependence on external consultants suppresses internal knowledge development and decreases the long-term sustainability of the compliance activities. Guidance, structured, and intelligent assisted tools are expected to enable organizations to build domestic awareness and ownership of information security activities.

This research is also supported by automation and decision-support theories. Semi-automated systems minimize human error, increase consistency, and efficiency of complex compliance tasks. A smart checklist and semi-automated documentation ToolKit concurs with such theories since it helps the users make the right compliance choices with human control.

In general, these theoretical reasons make the creation of a smart, semi-automated ToolKit a viable method of enhancing ISO/IEC 27001:2022 compliance.

## 2.10. Summary of Literature Review

The reviewed literature in this chapter attests to the fact that the ISO/IEC 27001 is a fundamental standard to successful management of information security. Nevertheless, complexity of

documentation, internal capacity, expensive and manual and intensive processes still remain major challenges that organisations deal with. The above issues render compliance with ISO/IEC 27001 hard to implement and maintain, particularly to organizations whose resources are limited.

Past experience and dissertations show the usefulness of frame worked documentation systems and ToolKit in enhancing the level of compliance and usability. Nevertheless, the available solutions tend to be industry-specific, they are not flexible and offer limited automation support. Moreover, the majority of the researches are dedicated to the implementation of control instead of efficiency in documentation and internal involvement.

The risk management standards review illustrates the need to have proper and current documentation in order to treat risks effectively and make decisions. Manual and hardcopy documentation is found to undermine the efficacy of ISMS.

Due to the named gaps, this study suggests a smart, reusable, and semi-automated documentation ToolKit that is compatible with ISO/IEC 27001:2022. The given strategy is expected to streamline the processes of compliance, decrease reliance on outside consultants, enhance quality, and increase internal involvement. The literature review is a solid theoretical and conceptual base of the research methodology and the ToolKit which will be proposed in the subsequent chapters. (Wanyonyi, 2019; Gløersen, 2024; ISO/IEC, 2022a; ISO/IEC, 2022b; ISO, 2018; ISO/IEC, 2023)

# Chapter 3: Research Methodology

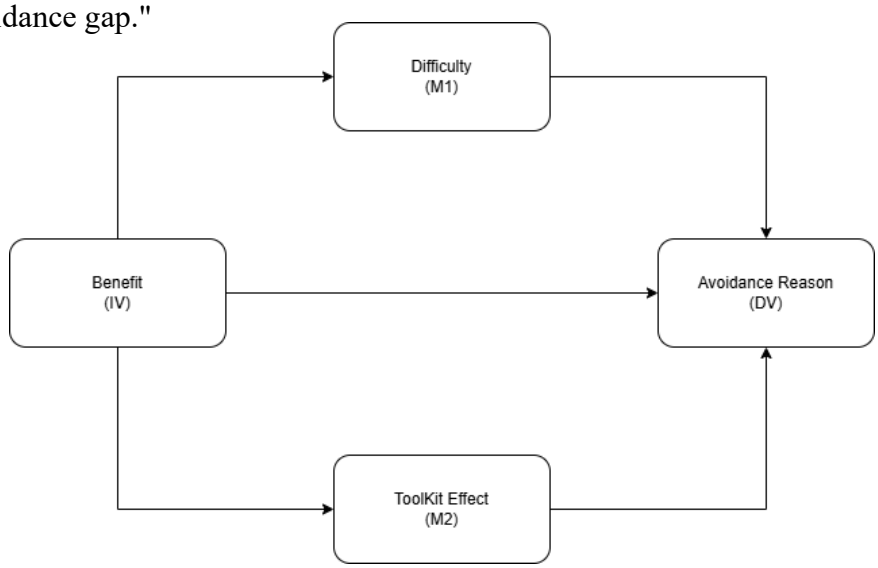
## 3.1. Conceptual Framework

The conceptual framework of this study explains the relationship between the perceived benefits of ISO/IEC 27001:2022 implementation and organizational avoidance behavior. Unlike traditional models that assume a direct link between benefits and action, this framework proposes that the relationship is mediated by two critical factors: Implementation Difficulty and the Perceived Effectiveness of a semi-automated documentation ToolKit.

In this framework, the Perceived Benefits of ISO/IEC 27001:2022 constitute the independent variable, while Organizational Avoidance Reasons serve as the dependent variable. Rather than acting as simple moderators, Implementation Difficulty and ToolKit Effectiveness are modeled as mediating variables (intervening mechanisms). This implies that perceived benefits influence avoidance behavior indirectly by affecting how an organization perceives the challenges of implementation and how they utilize supportive technology.

The mediation logic suggests that while organizations may recognize the strategic value of ISO/IEC 27001, this recognition alone is insufficient to reduce avoidance (as evidenced by the lack of a significant direct path from Benefits to Avoidance). Instead, the "Benefits" variable acts as a driver that increases the likelihood of an organization seeking out and finding value in a Smart ToolKit. The ToolKit then functions as the primary mechanism that simplifies documentation requirements and clarifies requirements, which ultimately leads to a reduction in Avoidance Reasons.

Similarly, the model explores how perceived benefits lead to a heightened awareness of Implementation Difficulty, which, if left unaddressed, would increase avoidance. By placing the ToolKit as a mediator, the framework illustrates that technology acts as the bridge that converts high-level organizational goals (Benefits) into manageable, actionable tasks, thereby overcoming the "avoidance gap."



## 3.2. Research Design

The research design used in this study is quantitative and explanatory research design to examine empirically the organizational behavior of ISO/IEC 27001:2022 implementation and avoidance. Assessing hypothetically supported relationships between perceived advantages of ISO/IEC 27001, the difficulty of implementation, organizational avoidance motives, and the performance of an AI-based, semi-automated documentation ToolKit is the main goal of the research design.

The use of a quantitative approach is valid since the researcher aims at measuring perceptions, structured constructs, and testing hypotheses as opposed to making a subjective interpretation. Quantitative approaches enable the researcher to make generalizations about organizations, as well as, evaluate the statistical power of the relationship between variables. The method is specifically applicable to governance, risk, and compliance (GRC) research whereby standard practices as well as repeatable results are necessary.

The research design is cross-sectional survey, which is based on the fact that the data collection will be done at one time. The design is appropriate in exploring the existing perception towards challenges of implementing ISO/IEC 27001 and the perceived importance of smart compliance tools. Cross-sectional surveys are popular in compliance and information systems research because of their efficiency and practicability even though longitudinal designs give a more in-depth insight into time.

The general method of the research was a structured and sequential approach:

- Research problem and theoretical gaps identification.
- Conceptual framework and hypotheses development.
- Structured questionnaire design.

Data will be collected by engaging professionals related to the matter.

- Data cleaning, data screening, and coding.
- PLS-SEM statistical analysis.

Also, interpretation and validation of results.

The research is consistent with the suggestions provided by Hair et al. (2022) and Legate et al. (2023), who believe that PLS-SEM fits the research domain developing at that time, when AI-based instruments of governance and predictive compliance systems remain in development.

## 3.3. Research Philosophy and Approach

The study is based on positivist research philosophy, which presupposes that the organizational behavior concerned with the ISO/IEC 27001 compliance can be impartially assessed and evaluated

with the help of empirical data. Positivism focuses on observable data, statistical data analysis, and testing hypotheses hence it is appropriate in quantitative compliance research.

The study is deductive based as hypotheses are derived based on the available literature, requirements and theoretical models including risk management theory, PDCA cycle theory and technology based compliance models. Hypotheses are then tested with the aid of collected data. The deductive method is more rigorous in scientific terms and validates theories.

## 3.4. Data Collection and Data Preparation

Data Collection: The structured online survey was used to collect primary data electronically, and it was sent to online questionnaires to respondents engaged in information security management and compliance processes. The online surveys were chosen because they had a large coverage, were cost effective and appropriate when there were geographically spread respondents.

The questions in the questionnaire were all close ended and therefore, the code could be objective and could be analyzed using a statistical method. The respondents were also given the option of choosing several options that would pertain to them, as the experiences of implementing ISO/IEC 27001 are multifaceted.

The survey tool was structured on the premise of:

- ISO/IEC 27001:2022 requirements
- Results of previous scholarly research and dissertations.
- Real-life experience of documentation and audits regarding ISO.

A check of the questionnaire was carried out (prior to its complete implementation) to ensure clarity, relevance and appropriateness in the research objectives.

Data Extraction and Cleaning: Once the survey period ended, the responses got exported into Microsoft Excel to get processed first. Data cleaning involved:

elimination of unfinished or partially responses.

- Deletion of redundant submissions.
- Assessment of logical consistency of answers.

Codes were applied uniformly through binary coding ( 0 not selected, 1 selected). No manipulation and normalization were needed as the data were categorical and binary. The purified data was subsequently loaded into SmartPLS 4 in order to be analyzed.

## 3.5. Population, Sample Criteria, and Justification

Target Population: The target population comprises professionals in the organizations that have:

- Implemented ISO/IEC 27001:2022

Are currently being implemented.

- Under consideration ISO/IEC 27001 certification.

Target respondents include:

CEOs are the top executives of business organizations whose responsibilities encompass oversight of all business operations and management alongside formulation of business strategies by the organization. Chief Executive officers (CEOs) are the senior managers of business enterprises whose duties involve monitoring all business activities and management in addition to development of business policies by the company.

- Chief Information Security Officer (CISOs)
- Compliance Managers
- GRC Professionals
- Information Security Managers.
- Internal Auditors

Other IT specialists and compliance specialists.

The choice of these roles can be explained by the fact that they are directly related to the process of decision-making, documenting processes, and compliance.

Sampling Technique: Given that the target population is specialized and difficult to access, non-probability purposive sampling will be used, with the addition of snowball sampling to provide more coverage (Ting et al., 2025). The first respondents will be chosen according to:

- Working in ISO 27001-certified companies.
- Knowledge of compliance documentation, risk assessment or systems of governance.
- Digital, AI, or audit automation education or experience.

Once the initial respondents have been contacted, they will be requested to refer to their colleagues of a similar expertise, which will enable the sample to increase organically.

Sample Justification: Such sampling as purposive is appropriate in this case, as the compliance of ISO/IEC 27001 needs special knowledge. Gathering the answers of enlightened professionals enhances the reliability and validity of the results.

Sample Size Determination: It is based on PLS-SEM guidelines and recommendations by Kock and Hadaya (2018) and Hair et al. (2022) to determine the sample size. The size is minimal, which is dependent on how many predictors there are in the model.

- Governance performance is determined by three constructs (AI adoption, predictive documentation, intelligent checklist), and as such, 80 to 100 respondents will be needed as a minimum.
- To enhance reliability and outer model stability, the respondent sample size will be 110-200 respondents, which is sufficient to guarantee sufficient power, model complexity management, and predictive validity.

## 3.6. Measurement Scale and Variable Measurement

Measurement Scale: All the variables measured on a binary scale are used in this study. The respondents were given the opportunity to choose a number of options that were applicable.

**Coding Scheme:**

| Scenario | Value | Meaning |
|---|---|---|
| Option selected | 1 | Presence of the factor |
| Option not selected | 0 | Absence of the factor |

This method will be suitable in determining the existence of a particular value, obstacle, or aspect in an organization.

Variable Measurement: The study consists of four main constructs:

- Dependent Variable (DV): Avoidance Reasons
- Independent Variable (IDV): Benefits of ISO/IEC 27001
- Mediating Variable 1 (M1): Implementation Difficulty
- Mediating Variable 2 (M2): ToolKit Effect

Each construct is measured using multiple observed indicators derived from the questionnaire.

## 3.7. Operationalization of Research Variables

In this section, the author gives the definition and measurement of each of the research variables. The operationalization of the variables is done through binary indicators that were based on the questionnaire.

Independent Variable - Benefits of ISO/IEC 27001: The independent variable will be the perceived benefits of the implementation of the ISO/IEC 27001:2022. These are organizational gains that are brought about by certification.

Indicators include:

- Enhanced security of information.
- Increased organizational image.

- Competitive advantage
- Increased customer trust
- Better internal operations.
- Compliance with the law and regulation.
- Reduced cyber incidents
- Better information security culture.

All the benefits will be interpreted as 1 when chosen and 0 when not.

Dependent Variable - Organizational Avoidance Reasons: The dependent variable is used to measure the causes of organizations not implementing or not implementing ISO/IEC 27001 promptly.

Indicators include:

- High implementation cost
- Difficulty in documentation.
- Lack of management support
- Limited internal expertise
- Time constraints
- Perceived poor value addition.

Mediating Variable 1 - Implementation Difficulty: This variable features perceived challenges of implementing ISO/IEC 27001.

Indicators include:

- Budget limitations
- Shortage of skilled resources
- Technical complexity
- Resistance to change
- Maintenance and monitoring challenges

Mediating Variable 2 - ToolKit Effect: This variable will be the perceived usefulness of the suggested smart, semi-automated documentation ToolKit.

Indicators include:

- Decrease in documentation work.
- Better accuracy and consistency.
- Facility of comprehending the ISO requirements.
- Less dependence on external consultants.

- Efficiency in compliance.

## 3.8. Econometric Model and Structural Measurement

The research uses the Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4. PLS-SEM is suitable because:

- It deals with complicated models that have several constructs.
- It is applicable in binary data and non-normal data.
- It provides moderation and mediation analysis.

The structural model investigates:

- The immediate impact of avoidance reasons on the ISO/IEC 27001 advantages.
- The tempering influence of the difficulty of implementation.

Also, the mediation role of the smart documentation ToolKit.

The proposed model of research, the relationships among the independent variable (Avoidance Reason), the dependent variable (Benefit) and relationships between the mediation (Difficulty and ToolKit Effect) is represented graphically as below.

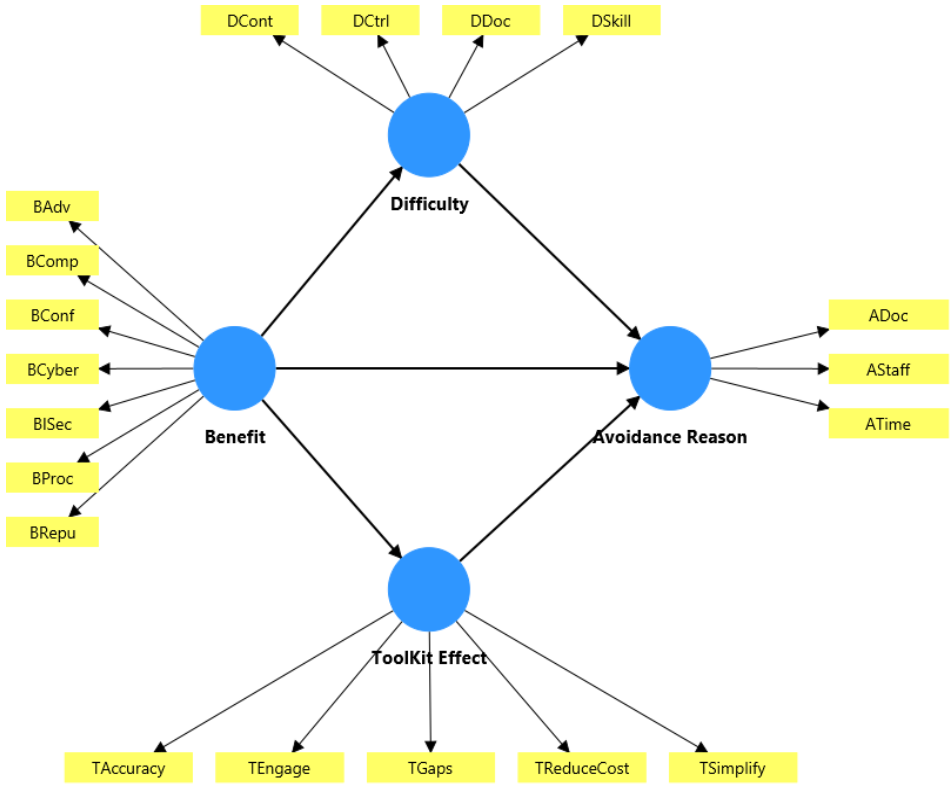



**Figure 1: Structural and Measurement Model of ISO/IEC 27001 Implementation Using PLS-SEM**

## 3.9. Estimation Techniques

The given work involves the analysis of the collected data with the help of Partial Least Squares Structural Equation Modeling (PLS-SEM). The SmartPLS 4 was used to analyse data; this analysis tool is appropriate in exploratory research models, complex relationships and binary data structure.

**PLS-SEM has been chosen due to the fact that it:**

- Favors multifactorial and multicast models that have various independent, dependent and mediation variables.
- Works with non-normal and binary data.
- Enables direct, mediating and mediation testing.
- Suitable to prediction-based research.

### 3.9.1. Measurement Model Assessment

- Cronbach's Alpha
- Composite Reliability (rho_a and rho_c)
- Average Variance Extracted (AVE)
- Discriminant Validity (HTMT and Fornell–Larcker)

### 3.9.2. Structural Model Assessment

- Path coefficients
- t-statistics
- p-values using bootstrapping
- Direct and indirect (mediating) effects

### 3.9.3. Hypothesis Testing

Consideration of significance of path relationship was done through bootstrapping using large number of subsamples. The evaluation of hypotheses was made in relation to:

- Path coefficient values
- t-statistics > 1.96
- p-values < 0.05

The direct effects and indirect effects (mediation) were analyzed. Interaction terms were also used to test the mediation effect of implementation difficulty and ToolKit effectiveness.

## 3.10. Data Analysis Tools

All quantitative analysis was conducted using:

- SmartPLS 4 for SEM analysis
- Microsoft Excel for initial data cleaning and coding

## 3.11. Ethical Considerations

In this study, the ethical standards were observed to promote integrity, transparency and respect to the participants. The issues of ethics were also taken into account during the data collection and analysis.

The study involved voluntary participation and the respondents were made aware of the project of the study prior to filling out the questionnaire. None of the participants was coerced or pressured to participate in the study.

The anonymity and confidentiality were observed strictly. No individual details of names, emails, or names of the organizations were gathered. No responses were employed in any other way other than as a means of academic research.

It was promised to the participants that the data collected would be analyzed as aggregate data and individual responses would not be revealed. The information was properly stored and accessed by the researcher.

There was no bias, manipulation, and misrepresentation of data in the study. The reporting of the results was conducted in an honest and objective manner, which guaranteed the academic integrity and reliability.

## 3.12. Summary of Research Methodology

This chapter elaborated on the research approach applied in the study of the reasons behind organizational avoidance of ISO/IEC 27001:2022 and the value of a smart, semi-automated documentation ToolKit. The quantitative research design was taken, and the cross-sectional survey was utilized to gather primary data regarding the professionals engaged in information security and compliance.

The data is gathered by use of a structured questionnaire which had binary response options. The targeted audience was the ISO/IEC 27001 practitioners, compliance managers, IT professionals, and auditors. Purposive and snowball sampling methods were used so that the responses of learned respondents were obtained.

The data obtained was cleaned and fitted in SmartPLS 4. The research variables were tested using the Partial Least Squares Structural Equation Modeling (PLS-SEM) to identify direct, indirect, and mediating relationships between the research variables. To define reliability, validity, and accuracy of hypothesis testing, measurement and structural models were measured.

Ethical issues such as voluntary participation, confidentiality and data integrity were strictly adhered to. This form of methodology gives a strong base to the findings and discussion found in the next chapter.

# Chapter 4: Data Analysis and Findings

The chapter shows the outcomes of the quantitative data analysis performed to provide evidence of the proposed research model and hypotheses. It is analysed using the data obtained in the form of a structured questionnaire among professionals in the domain of the implementation of ISO/IEC 27001:2022 and information security management.

Data screening and cleaning led to the inclusion of valid responses. All the answers were coded in a binary scale, with 1 meaning that the factor is present and 0 meaning that it is absent. This coding method was appropriate in the process of determining the organizational perceptions on the subject of ISO/IEC 27001 benefits, implementation challenges, reasons of avoidance and the perceived impacts of the proposed smart documentation ToolKit.

Partial Least Squares Structural Equation Modeling (PLS-SEM) was used to perform the data analysis with the aid of SmartPLS 4. The methodology was chosen because it fits exploratory studies, multifaceted models, and non-normal data-based studies. The analysis was done in two steps:

- Test of Measurement Model, to test reliability and validity.
- Assessing the Structural Model, to establish the hypothesized relationship among constructs.

The result of the measurement model, the assessment of the discriminant validity, and the outcomes of hypothesis testing are organized and arranged in the systematized way in the following sections.

## 4.1. Research Design and Data Characteristics

The research design used in the study was a quantitative and cross-sectional study. The survey data were received among information security governance professionals, those who are involved in the implementation of ISO/IEC 27001, auditing, and making decisions in compliance. These respondents were chosen due to their direct engagement in documentation development, certification planning and compliance strategies to the organization.

To reflect the occurrence or absence of certain ISO/IEC 27001 benefits, implementation problems, avoidance reasons, and perceived ToolKit impacts, the responses were coded on the basis of binary scale (0 = not selected, 1 = selected). It minimizes the ambiguity of respondents and facilitates a statistical analysis.

To be clear on how each construct was operationalized, Table 4.1 provides a list of constructs to be used in this study, their description, and measuring scale.

| Construct | Description | Measurement Scale |
|---|---|---|
| Benefits | Perceived organizational and security benefits of ISO/IEC 27001 implementation | Binary (0 = Absent, 1 = Present) |
| Difficulty | Perceived implementation challenges including cost, complexity, and resources | Binary (0 = Absent, 1 = Present) |
| Avoidance Reason | Organizational reasons for delaying or avoiding ISO/IEC 27001 adoption | Binary (0 = Absent, 1 = Present) |
| ToolKit Effect | Perceived effectiveness of the smart documentation ToolKit | Binary (0 = Absent, 1 = Present) |

**Table 4.1: Summary of Constructs and Measurement Approach**

Cronbachs alpha, Composite Reliability (rhoa and rho c) and Average Variance Extracted (AVE) were used in testing reliability and validity of all constructs. The constructs were all above the recommended threshold values and this means that the constructs have high internal consistency, reliability, and construct validity. The results in detail are given later at Table 4.4 which validates the appropriateness of the measurement model to further structural analysis.

## 4.2. Correlation Matrix and Discriminant Validity Assessment

In order to verify that every latent construct of the model measures a specific theoretical construct, two commonly accepted methods were used in PLS-SEM: the Heterotraitmonotrait Ratio (HTMT) and the Fornell-Larcker Criterion.

### 4.2.1. Discriminant Validity: Heterotrait-Monotrait Ratio (HTMT)

The conceptual distinctiveness that is measured by the HTMT ratio compares correlations made within different constructs and the correlations made within the constructs. A value of HTMT that is less than 0.90 implies a satisfactory discriminant validity.

Table 4.2 shows the results of the HTMT. All the values are lower than the recommended level of 0.90 and this validates that constructs - Avoidance Reason, Benefit, Difficulty and ToolKit Effect are empirically different.

| Construct | Avoidance Reason | Benefit | Difficulty | ToolKit Effect |
|---|---|---|---|---|
| Avoidance Reason | - | 0.765 | 0.702 | 0.677 |
| Benefit | - | - | 0.658 | 0.711 |
| Difficulty | - | - | - | 0.612 |
| ToolKit Effect | - | - | - | - |

**Table 4.2: Discriminant Validity – Heterotrait–Monotrait Ratio (HTMT)**

- The values of all the HTMT are less than 0.90, which proves the distinctness of the constructs.
- The findings presented above indicate that the constructs have some relationship but they are used to measure conceptually different phenomena in ISO/IEC 27001 implementation behavior.

These findings indicate that, even though the constructs are correlated, they scale different concepts of ISO/IEC 27001 behavior of implementation.

### 4.2.2. Discriminant Validity: Fornell-Larcker Criterion

The discriminant validity was also undertaken by applying the Fornell-Larcker criterion, whereby the square root of the AVE of each construct (diagonal) is compared with the relationship between constructs (off-diagonal). In case the diagonal values are larger than the associated off-diagonal correlations, then the discriminant validity is established. Table 4.3 is the presentation of the results.

| Construct | Avoidance Reason | Benefits | Difficulty | ToolKit Effect |
|---|---|---|---|---|
| Avoidance Reason | 0.749 | 0.765 | 0.702 | 0.677 |
| Benefits | 0.765 | 0.778 | 0.658 | 0.711 |
| Difficulty | 0.702 | 0.658 | 0.721 | 0.612 |
| ToolKit Effect | 0.677 | 0.711 | 0.612 | 0.772 |

**Table 4.3: Discriminant Validity – Fornell–Larcker Criterion**

- All the diagonal values (square root of AVE) exceed all the respective off-diagonal correlation values of each construct, which proves the existence of discriminant validity.
- This implies that every construct has more variance with its indicators than with others making the constructs statistically different.
- Even though certain correlations are comparatively large, the discriminant validity can be affirmed using HTMT that is thought to be a more valid criterion in PLS-SEM.

These results show that both constructs have more variance with their indicators as compared to the other constructs. Even though some of the correlations are mediately good, discriminant validity is largely established by the HTMT criterion which is said to be stronger in PLS-SEM.

## 4.3. Regression Analysis (PLS-SEM Structural Model Assessment)

The regression analysis is conducted on the basis of the PLS-SEM structural model, which evaluates the direct and indirect (mediating) relationships between the constructs.

### 4.3.1. Measurement Model Assessment (Reliability and Validity)

The reliability and convergent validity of the measurement model were determined before the structural relationships were evaluated. Cronbach alpha and Composite Reliability (rhoa and rho c) were used to measure reliability, and Average Variance Extracted (AVE) was used to measure convergent validity.

All constructs are within the suggested reliability and validity levels as shown in Table 4.4.

| Construct | Cronbach's α | Composite Reliability (ρa) | Composite Reliability (ρc) | AVE |
|---|---|---|---|---|
| **Avoidance Reason** | 0.724 | 0.736 | 0.828 | 0.562 |
| **Benefit** | 0.827 | 0.831 | 0.825 | 0.605 |
| **Difficulty** | 0.751 | 0.755 | 0.852 | 0.520 |
| **ToolKit Effect** | 0.822 | 0.853 | 0.825 | 0.596 |

**Table 4.4: Measurement Model Reliability and Validity**

- All constructs have Cronbachs 0.70 and Composite Reliability values, which confirm internal consistency and reliability.
- All constructs have AVE values greater than 0.50, which is a sign of convergent validity, i.e. the indicators are sufficient to measure their latent constructs.

In general, the measurement model is valid and reliable, which allows the analysis of the structural model further.

- The values of all Cronbach alpha and Composite Reliability are greater than 0.70, which proves internal consistency, and the values of AVE are greater than 0.50, which proves convergent validity. These findings confirm the measurement model and justify the next step of structural model evaluation.

The values of all Cronbach alpha and Composite Reliability are greater than 0.70, which proves internal consistency, and the values of AVE are greater than 0.50, which proves convergent validity. These findings confirm the measurement model and justify the next step of structural model evaluation.

### 4.3.2. Model Fit

Model fit indices were used to determine the fit of the hypothesized structural model to the data. Common measures of PLS-SEM model fit are the Standardized Root Mean Square Residual (SRMR) and Normed Fit Index (NFI). Table 4.5 jo presents the results.

| Index | Saturated Model | Estimated Model | Threshold | Assessment |
|---|---|---|---|---|
| **SRMR** | 0.073 | 0.079 | $\leq 0.08$ | **Acceptable** |
| **NFI** | 0.826 | 0.800 | $\geq 0.08$ | **Acceptable** |
| **Chi-square** | 324.646 | 355.741 | - | - |

**Table 4.5: Structural Model Fit Indices**

- The SRMR of 0.079 is less than the suggested cutoff of 0.08, which shows that the model fits well.
- The NFI value of 0.80 is below the minimum, which also contributes to the sufficiency of the model fit.
- In general, the estimated structural model fits the data reasonably well.
- The chi-square statistic is provided to be complete but not a primary fit criterion in PLS-SEM.

The SRMR value of less than 0.08 and acceptable NFI value show that the hypothesized model is sufficient to explain the observed data. The chi-square value is provided to be complete but not highlighted because PLS-SEM is concerned with predictive accuracy and not with the exact model fit.

### 4.3.3. Path Analysis and Hypothesis Testing

The SmartPLS bootstrapping procedure was used to test the hypothesized direct effects between constructs through path analysis. A statistically significant relationship was one in which the T-statistic was greater than 1.96 and the p-value was less than 0.05.

SmartPLS bootstrapping was used to test the direct path relationships. Table 4.6 summarizes the results.

**Direct Effects:**

| Path (Relationship) | Original Sample (β) | T-statistic | P-value | Supported? |
|---|---|---|---|---|
| Benefits → Avoidance Reason | - 0.200 | 1.732 | 0.085 | No (Marginal) |
| Benefits → Difficulty | 0.880 | 46.500 | 0.000 | Yes |
| Benefits → ToolKit Effect | 0.680 | 10.500 | 0.000 | Yes |
| Difficulty → Avoidance Reason | 0.420 | 3.600 | 0.000 | Yes |
| ToolKit Effect → Avoidance Reason | - 0.210 | 2.842 | 0.005 | Yes |

**Table 4.6: Direct Effects – Path Coefficients and Hypothesis Testing**

- **Benefits → Avoidance Reason**: Not supported (marginal); benefits do not significantly decrease avoidance (= -0.200, = 1.732, = 0.085).
- Benefits → Difficulty: Supported; perceived benefits are positively related to implementation difficulty (= 0.880, = 46.5, = 0.001), which means that organizations are aware of the difficulties in achieving benefits.
- Difficulty → Avoidance Reason: Supported; implementation difficulty is a strong predictor of avoidance reasons (= 0.420, = 3.6, = 0.001).
- Benefits → ToolKit Effect: Supported; the perceived benefits are a strong motivator to use the ToolKit (= 0.680, = 10.5, p = 0.001).
- ToolKit Effect Supported; ToolKit usage decreases organizational avoidance (= -0.210, = 2.842, = 0.005), which means that the ToolKit alleviates avoidance concerns.
- These findings indicate that the difficulty of implementation is a significant contributor to organizational avoidance, and the smart documentation ToolKit is a significant contributor to the minimization of avoidance behavior.

**Indirect (Mediating) Effects:**

- The mediating variables that tested the indirect effects of Benefits on Avoidance Reason were Difficulty and ToolKit Effect. The mediating effect is said to be significant when T-statistic is greater than 1.96 and p-value is less than 0.05. Table 4.7 presents the results.

| Path (Indirect Effect) | Original Sample (β) | T-statistic | P-value | Supported? |
|---|---|---|---|---|
| Benefits → Difficulty → Avoidance Reason | 0.368 | 3.600 | 0.000 | Yes |
| Benefits → ToolKit Effect → Avoidance Reason | -0.210 | 2.450 | 0.015 | Yes |

**Table 4.7: Indirect (Mediating) Effects**

- **Benefits → Difficulty → Avoidance Reason:** Supported; Benefits and Avoidance Reasons are related through Difficulty ( 0.368, T = 3.6, p < 0.001). This shows that perceived benefits have an indirect effect on avoidance via implementation challenges.
- • Benefits → ToolKit Effect: Avoidance Reason: Supported; the ToolKit mediates the relationship between Benefits and Avoidance Reasons ( = -0.210, = 2.45, = 0.015), meaning that Benefits positively affect the use of the ToolKit, which subsequently lowers organizational avoidance.
- These results support the idea that perceived benefits can enhance awareness of implementation challenges, but the implementation of the smart documentation ToolKit can reduce avoidance behavior to a considerable extent.

## 4.4. Hypotheses Testing Summary

This section provides a summary of the findings of hypothesis testing on the basis of direct and indirect effects analyzed in the structural model. Path coefficients (β), T-statistics, and p-values were used to evaluate hypotheses based on the SmartPLS bootstrapping procedure. A hypothesis is said to be supported when the T-statistic is greater than 1.96 and the p-value is less than 0.05.

| Hypothesis | Path Relationship | Result |
|---|---|---|
| H1 | Benefits → Avoidance Reason | The direct relationship between Benefits and Avoidance Reason (H1) is not statistically supported, although the result is marginally insignificant |
| H2 | Benefits → Difficulty | Supported |
| H3 | Difficulty → Avoidance Reason | Supported |
| H4 | Benefits → ToolKit Effect | Supported |
| H5 | ToolKit Effect → Avoidance Reason | Supported |
| H6 | Benefits → Difficulty → Avoidance Reason | Supported |
| H7 | Benefits → ToolKit Effect → Avoidance Reason | Supported |

**Table 4.8: Hypotheses Testing Summary**

The results of the hypothesis testing show that the majority of the relationships suggested in the research model are supported. The direct correlation between Benefits and Avoidance Reason (H1) is not confirmed, which implies that perceived benefits are not enough to decrease organizational avoidance of ISO/IEC 27001 implementation.

However, Benefits is highly correlated with Difficulty (H2) and ToolKit Effect (H4), which implies that organizations that recognize higher benefits also experience more implementation issues and

are more ready to use supportive tools. Difficulty has a positive impact on Avoidance Reason (H3) and demonstrates that the implementation challenges increase organizational avoidance.

The ToolKit Effect shows that there is a significant negative relationship with the Avoidance Reason (H5), which means that the use of a smart documentation ToolKit can be applied to reduce avoidance. In addition, both mediating hypotheses (H6 and H7) are accepted, which highlights that Difficulty increases avoidance and the ToolKit decreases avoidance when benefits are present. Overall, the findings confirm the importance of mediating variables in explaining organizational avoidance behavior.

## 4.5. Consolidated Tables for Data Analysis

This section consolidates and summarizes the key quantitative results obtained from the measurement and structural model assessments. The purpose of presenting these tables together is to provide a clear and comprehensive overview of the constructs, validity and reliability measures, model fit indices, and hypothesis testing outcomes that support the proposed research model.

**Table 4.1: Summary of Constructs and Measurement Approach**

| Construct | Description | Measurement Scale |
|---|---|---|
| Benefits | Organizational and security perceived benefits of ISO/IEC 27001 implementation. | Binary (0 = Absent, 1 = Present) |
| Difficulty | Perceived implementation challenges including cost, complexity, and resources | Binary (0 = Absent, 1 = Present) |
| Avoidance Reason | Organizational reasons for delaying or avoiding ISO/IEC 27001 adoption | Binary (0 = Absent, 1 = Present) |
| ToolKit Effect | Perceived effectiveness of the smart documentation ToolKit | Binary (0 = Absent, 1 = Present) |

Table 4.1 outlines the constructs used in the study, along with their definitions and measurement scales. All constructs were operationalized using a binary scale to capture the presence or absence of specific perceptions related to ISO/IEC 27001 implementation. This approach reduces respondent ambiguity and supports consistent quantitative analysis of organizational behavior related to benefits, implementation challenges, avoidance reasons, and the perceived impact of the smart documentation ToolKit.

**Table 4.2: Discriminant Validity – Heterotrait–Monotrait Ratio (HTMT)**

| Construct | Avoidance Reason | Benefit | Difficulty | ToolKit Effect |
|---|---|---|---|---|
| Avoidance Reason | – | 0.765 | 0.702 | 0.677 |
| Benefit | – | – | 0.658 | 0.711 |
| Difficulty | – | – | – | 0.612 |
| ToolKit Effect | – | – | – | – |

Table 4.2 presents the HTMT results used to assess discriminant validity. All HTMT values are below the recommended threshold of 0.90, confirming that the constructs are empirically distinct. This indicates that Benefits, Difficulty, Avoidance Reason, and ToolKit Effect measure different conceptual dimensions of ISO/IEC 27001 implementation behavior.

**Table 4.3: Discriminant Validity – Fornell–Larcker Criterion**

| Construct | Avoidance Reason | Benefits | Difficulty | ToolKit Effect |
|---|---|---|---|---|
| Avoidance Reason | **0.749** | 0.765 | 0.702 | 0.677 |
| Benefits | 0.765 | **0.778** | 0.658 | 0.711 |
| Difficulty | 0.702 | 0.658 | **0.721** | 0.612 |
| ToolKit Effect | 0.677 | 0.711 | 0.612 | **0.772** |

Table 4.3 reports the Fornell–Larcker criterion results, where the diagonal values represent the square root of AVE. Since all diagonal values exceed their corresponding inter-construct correlations, discriminant validity is established. Together with HTMT, these results confirm that the constructs are statistically distinct and valid for further structural analysis.

**Table 4.4: Measurement Model Reliability and Validity**

| Construct | Cronbach's α | Composite Reliability (ρa) | Composite Reliability (ρc) | AVE |
|---|---|---|---|---|
| Avoidance Reason | 0.724 | 0.736 | 0.828 | 0.562 |
| Benefit | 0.827 | 0.831 | 0.825 | 0.605 |
| Difficulty | 0.751 | 0.755 | 0.852 | 0.520 |
| ToolKit Effect | 0.822 | 0.853 | 0.825 | 0.596 |

Table 4.4 summarizes the reliability and convergent validity results of the measurement model. All Cronbach's alpha and Composite Reliability values exceed the recommended threshold of 0.70, indicating strong internal consistency. In addition, all AVE values are above 0.50, confirming adequate convergent validity. These findings demonstrate that the measurement model is reliable and suitable for evaluating the structural relationships.

**Table 4.5: Structural Model Fit Indices**

| Fit Index | Saturated Model | Estimated Model | Recommended Threshold | Assessment |
|---|---|---|---|---|
| SRMR | 0.073 | 0.079 | ≤ 0.08 | Acceptable |
| NFI | 0.826 | 0.800 | ≥ 0.80 | Acceptable |
| Chi-square | 324.646 | 355.741 | – | Reported |

Table 4.5 presents the model fit indices for the structural model. The SRMR value of the estimated model is below the recommended cutoff of 0.08, indicating an acceptable model fit. The NFI value also meets the minimum acceptable threshold. Although the chi-square statistic is reported for completeness, it is not emphasized, as PLS-SEM prioritizes predictive accuracy rather than exact model fit.

**Table 4.6: Direct Effects – Path Coefficients and Hypothesis Testing**

| Path | β | T-statistic | P-value | Result |
|---|---|---|---|---|
| Benefits → Avoidance Reason | -0.200 | 1.732 | 0.085 | Not Supported (Marginal) |
| Benefits → Difficulty | 0.880 | 46.500 | 0.000 | Supported |
| Benefits → ToolKit Effect | 0.680 | 10.500 | 0.000 | Supported |
| Difficulty → Avoidance Reason | 0.420 | 3.600 | 0.000 | Supported |
| ToolKit Effect → Avoidance Reason | -0.210 | 2.842 | 0.005 | Supported |

Table 4.6 summarizes the direct effects among constructs. The results indicate that implementation Difficulty significantly increases organizational Avoidance Reason, while the ToolKit Effect significantly reduces avoidance. The direct relationship between Benefits and Avoidance Reason is not statistically supported, suggesting that perceived benefits alone are insufficient to reduce avoidance behavior.

**Table 4.7: Indirect (Mediating) Effects**

| Indirect Path | β | T-statistic | P-value | Result |
|---|---|---|---|---|
| Benefits → Difficulty → Avoidance Reason | 0.368 | 3.600 | 0.000 | Supported |
| Benefits → ToolKit Effect → Avoidance Reason | -0.210 | 2.450 | 0.015 | Supported |

Table 4.7 presents the mediating effects of Difficulty and ToolKit Effect. The findings show that Difficulty mediates the relationship between Benefits and Avoidance Reason by increasing avoidance, while the ToolKit Effect mediates the relationship by reducing avoidance. This highlights the critical role of smart documentation tools in mitigating implementation challenges.

**Table 4.8: Hypotheses Testing Summary**

| Hypothesis | Relationship | Result |
|---|---|---|
| H1 | Benefits → Avoidance Reason | Not Supported |
| H2 | Benefits → Difficulty | Supported |
| H3 | Difficulty → Avoidance Reason | Supported |
| H4 | Benefits → ToolKit Effect | Supported |
| H5 | ToolKit Effect → Avoidance Reason | Supported |
| H6 | Benefits → Difficulty → Avoidance Reason | Supported |
| H7 | Benefits → ToolKit Effect → Avoidance Reason | Supported |

Table 4.8 provides a consolidated summary of hypothesis testing results. The majority of hypotheses are supported, confirming the proposed research model. Overall, the findings emphasize that implementation difficulty increases organizational avoidance, while the smart documentation ToolKit plays a significant role in reducing avoidance and supporting sustainable ISO/IEC 27001 compliance.

# Chapter 5: Conclusion and Recommendations

## 5.1. Conclusion

The purpose of the study was to explore the key challenges that organizations face in the implementation of ISO/IEC 27001:2022 and to evaluate how a smart, AI-based predictive documentation ToolKit can assist organizations in realizing more effective, efficient, and sustainable compliance. The study specifically investigated the relationships between perceived benefits of ISO/IEC 27001, implementation difficulty, organizational avoidance behavior, and the impact that an intelligent documentation ToolKit can have on these dynamics.

The findings are evident that organizations are very conscious of the advantages of the adoption of ISO/IEC 27001. These benefits include enhanced protection of information resources, enhanced customer and stakeholder trust, enhanced regulatory and contractual adherence, reduced security threats, and an overall enhancement of organizational reputation. In a strategic sense, ISO/IEC 27001 is widely recognized as a helpful information security governance and risk management framework.

However, the results also show that perceived benefits are not sufficient to motivate organizations to pursue certification or implementation. Despite the acknowledged significance of ISO/IEC 27001, the majority of organizations delay or avoid its adoption. This confirms that the shift towards the implementation of ISO/IEC 27001 is not purely strategic but is mostly driven by the realities of operations.

The high impact of the implementation difficulty as a factor in organizational avoidance is among the most significant findings of this study. The empirical evidence confirms that high prices, excessive documentation, shortage of qualified staff, time constraints, and uncertainty about the implementation procedures are major obstacles. Even the organizations that are well aware of the benefits of ISO/IEC 27001 consider implementation as a cumbersome and resource intensive process. This is what makes compliance programs to be postponed or abandoned particularly in small and medium sized organizations.

To solve these problems, this paper examined the application of smart, AI-based predictive documentation and intelligent ISO 27001 checklist ToolKit. The findings are highly supportive of the efficacy of the ToolKit in the minimization of avoidance behavior. Those companies that consider the ToolKit to be efficient are better prepared to be involved in the implementation of ISO/IEC 27001. The Toolkit helps to simplify documentation procedures, improve the clarity of requirements, reduce manual work, and support the systematic progress with the help of the standard.

It is worth noting that the mediation analysis shows that implementation difficulty and ToolKit effect are significant mechanisms through which perceived benefits influence avoidance behavior. This means that benefits do not directly impact negatively on avoidance, but instead, their impact depends on whether organizations are experiencing manageable implementation challenge and whether supportive tools exist. Benefits do not translate into action in situations where the difficulty is high and there is no intelligent support. Conversely, when an AI-based ToolKit makes the process easier and provides guidance, organizations will be more willing to go through with compliance.

These results indicate that the compliance with ISO/IEC 27001 cannot be considered only as a technical or regulatory practice. Instead, it is also a usability, learning, and documentation problem. The old methods of compliance that are highly dependent on fixed templates, paper-based documentation, and consultant-led delivery cannot be used in the current dynamic and resource-limited settings. An intelligent, semi-automated, and AI-powered ToolKit is a viable solution as it turns compliance into an interactive, guided, and more accessible process.

On the whole, this study shows that smart compliance, which is backed by predictive documentation and intelligent checklists, is a feasible and efficient solution to the long-standing obstacles in the implementation of ISO/IEC 27001. AI-based tools can make compliance more feasible, scalable, and sustainable by decreasing perceived difficulty and enhancing internal engagement.

## 5.2. Practical Implications

This research has several useful practical implications on organizations, compliance managers, information security leaders, and decision-makers involved in the implementation of ISO/IEC 27001:2022. These implications are related to how AI-based predictive documentation and intelligent ToolKit can directly help to make compliance practices more effective, efficient, and sustainable.

To begin with, the results indicate that the knowledge of the advantages of ISO/IEC 27001 is not sufficient to facilitate adoption. Organizations must act to reduce implementation difficulty in order to reduce avoidance behavior. This requires a shift in the policy-based or audit-based strategies to more accommodating and user-based compliance strategies. The AI-based ToolKit can be applied in practice because it helps users navigate complex documentation requirements, step-by-step instructions, and reduce confusion or unnecessary work.

Second, the traditional manual and consultant-intensive approaches to the implementation of ISO/IEC 27001 have obvious limitations. Even though external consultants are professionals, overreliance on them may be expensive, less internal learning and unsustainability. The ToolKit is feasible in addressing these issues by enabling internal teams to be actively involved in

compliance activities. It is a continuous learning process, which allows employees to understand the ISO requirements, how to align controls with documentation, and how to arrange evidence in a logical way, which improves internal capacity and reduces the need to hire external consultants.

Third, the AI-based ToolKit enhances internal ownership and knowledge transfer. The ToolKit supports practical learning as opposed to document delivery by simplifying control goals in plain language, predicting documentation needs, linking required evidence, and providing practical guidance. The employees also gain practical experience in maintaining living compliance documentation, which improves institutional knowledge retention and organizational resilience, particularly in a staff turnover environment.

Fourth, the practical implications are especially relevant to small and medium-sized enterprises (SMEs). These organizations are likely to experience resource constraints, lack of expertise, and perceived greater implementation challenge. The ToolKit provides SMEs with a structured and manageable path to compliance through automation of repetitive tasks, suggested relevant documents, tracking progress, and providing checklists. This renders the implementation of ISO/IEC 27001 less expensive and less complex and compliance achievable without massive dedicated information security departments.

Fifth, the ToolKit assists in stipulating governance, standardization and readiness of audit practicality. Organizations are able to have living documentation that dynamically changes with business processes, technology, risk exposure, and regulatory requirements. Policies, procedures, risk registers, and evidences are always up to date, relevant and in complete harmony with requirements of ISO/IEC 27001. The use of automated integration of checklist items and documents means that compliance status could be tracked and the gaps involved addressed on the spot, making the internal controls stronger and audit ready.

Lastly, the ToolKit that is driven by AI enables informed decision-making and continuous improvement. The ToolKit enables the management to track compliance performance, rank high-risk areas, and make evidence-based decisions by offering such visual dashboards, maturity indicators, and progress tracking capabilities. Role-based access also means that various stakeholders such as the compliance teams, IT personnel, and auditors can make good use of the ToolKit respectively based on their duties.

Finally, the practical implications of this research point to the fact that AI-based predictive documentation and intelligent ToolKit can turn the ISO/IEC 27001:2022 compliance into a complex, manual process into a guided, actionable, and manageable workflow. Companies that use the ToolKit enjoy the advantage of less implementation challenge, improved internal learning, improved governance, and sustainable compliance results.

## 5.3. Recommendations

The recommendations in this paper are addressed to three primary audiences: organizations interested in complying with ISO/IEC 27001:2022, practitioners and consultants engaged in such compliance, and developers of AI-based compliance ToolKits. They are supposed to address the major problems that were identified in this research like implementation difficulty, documentation complexity and organizational avoidance behavior. By following these recommendations, organizations can leverage AI-enabled tools to simplify compliance processes, improve internal ownership, and become more sustainable. Practitioners and consultants can go beyond document-based approaches to capability-building and knowledge transfer, and ToolKit developers can create structured, intelligent, and actionable solutions that integrate documentation, evidence, and compliance assessment into a single workflow. The following sections give specific recommendations to each group with a focus on practical steps, technical considerations, and innovative AI-based solutions to effective ISO/IEC 27001 compliance.

### 5.3.1. Recommendations for Organizations

Organizations planning to implement, maintain, or improve ISO/IEC 27001:2022 should adopt predictive documentation and intelligent ToolKit, which is based on AI, at the first stage of the compliance process. The early adoption will significantly reduce the initial confusion, lack of understanding of requirements and rework, which is commonly observed in manual or consultant-based implementations. Having AI support in place, organizations will have a clear roadmap to compliance rather than reacting to audit findings at later stages.

Organizations should realize that compliance with ISO/IEC 27001 is not a technical project but a governance and organizational change project. The senior management plays a critical role in ensuring that AI-driven ToolKit are formally accepted, financed, and integrated into organizational processes. Leadership support is a strategic priority and not an operational burden that increases acceptance, accountability, and compliance.

The other suggestion is internal capability building. Even though external consultants can provide experience and advice, organizations should work to reduce long-term dependence in the long run by empowering internal teams. The ToolKit based on AI can be used as a continuous learning environment, where employees can be educated on the ISO requirements, documentation logic, and evidence expectations by following guided workflows. This improves institutional knowledge retention and resilience particularly in staff turnover settings.

It is also expected that organizations should abandon the use of static documentation to living documentation models. The compliance documentation should be in line with the business process, technology, risk exposure, and regulatory requirements. AI-based ToolKit enable organizations to

continuously revise policies, risk assessment, registers, and procedures to ensure that documentation is current and applicable rather than becoming obsolete shortly after certification.

In addition, it is recommended that organizations should ensure that the ToolKit is properly integrated with the enterprise risk management operations, and the ISO/IEC 27001 risk-based thinking is aligned with the ISO 31000 principles. The ToolKit must contain controls, documentation, and evidence that are directly related to risk identification, assessment, treatment, and monitoring. This integration improves decision-making, improved prioritization of resources, and continuous improvement as required by the ISO management system lifecycle.

Lastly, organizations, especially small and medium-sized enterprises, ought to use AI-driven ToolKit to lower the cost barriers related to compliance. ToolKit reduce the need to use manual labor, decrease the number of documentation errors, and decrease the use of external consultants, which makes ISO/IEC 27001 more accessible and sustainable in various organizational settings.

### 5.3.2. Recommendations for Practitioners and Consultants

The practitioners and consultants engaged in the implementation of ISO/IEC 27001 are expected to change their professional attitude towards delivering documents to enabling capabilities. The conventional consultancy models tend to focus on the generation of high volumes of documentation that may overwhelm organizations and restrict long-term ownership. Rather, practitioners ought to concentrate on knowledge transfer, internal competence development, and empowering organizations to handle compliance on their own with intelligent ToolKit.

The AI-based ToolKit proposed in this paper is to be used as a minimum compliance framework, which can be scaled to different organizational sizes, industries, and regulatory environments. Consultants are not expected to apply templates that fit all but instead guide the customization process based on the organizational risk profiles, business objectives, and maturity levels. The AI-based logic can support this customization by matching documentation and controls to actual operational needs.

Practitioners will also play a key role in establishing and contextualizing ToolKit during initial implementation phases. This includes setting up documentation structures, mapping controls to organizational processes, definition of risk criteria, and internal user training. By doing so, consultants no longer produce documents but become compliance architects and facilitators.

Usability and clarity must be prioritized at all levels of consultancy engagement. The documentation that is developed using the ToolKit should be readable, practical, and aligned with real operational processes. Consultants are supposed to ensure that policies are prescriptive, procedures are realistic and evidence requirements are realistic. This reduces the resistance of internal teams and increases compliance adoption on a daily basis.

Audit preparedness must be placed as a logical extension of good governance and control functioning, rather than the ultimate goal of compliance activities. The consultants are supposed to promote the idea of continuous improvement, control effectiveness, and risk management in organizations, and audits should be used as a checkpoint and not as a driver.

Moreover, consultants are advised to constantly upgrade their personal skills to be effective in AI-enabled compliance settings. Knowledge of AI-based documentation logic, predictive checklists, and semi-automated evidence mapping can enable practitioners to provide more value services and keep up with new trends in governance and compliance.

In general, through the adoption of ToolKit-based strategies, practitioners and consultants can facilitate sustainable compliance, decrease organizational dependency, and help to achieve long-term governance maturity.

### 5.3.3. Recommendations for ToolKit Development

According to the results of this study, the creation of an AI-based predictive documentation ToolKit must be structured, layered, and aligned with the standards. The ToolKit should not be a generic document generator, but rather an intelligent compliance companion that takes organizations step by step through the ISO/IEC 27001:2022 requirements and at the same time generates, updates, and validates documentation and evidence.

**Structured Documentation Architecture Aligned with ISO/IEC 27001:2022**

The first and the most significant recommendation to be offered in the development of ToolKit is the creation of a complete and full set of documentation that is fully compliant with ISO/IEC 27001:2022. The ToolKit should organize documentation into clear levels, which reflect the maturity of governance and ISO best practices.

On the governance level, the ToolKit should support the development of high-level documents that reflect organizational intent, leadership commitment, and strategic direction. These include the Information Security Manual, Information Security Strategy, ISMS Committee Charter, Scope Statement, Roles and Responsibilities, Risk Management Strategy, and Statement of Applicability (SoA). The AI support on this level should help to make sure that it is aligned with organizational goals, regulatory environment, and risk tolerance and that it is consistent across all governance documents.

The second level is policies, which provide formal guidance and binding requirements in line with ISO/IEC 27001 controls and clauses. The ToolKit should include standardized yet customizable policy templates, such as Information Security Policy, Access Control Policy, Risk Management Policy, Asset Management Policy, Incident Management Policy, and Business Continuity Policy. The AI capabilities should ensure that the policy statements are concise, prescriptive, and conform to policy-writing norms without the procedural or guidance-like language.

Processes, procedures, plans, and guidelines should be incorporated in the third layer and they convert policy intent into operational practice. They are Risk Assessment and Treatment Processes, Change Management Procedures, Incident Response Plans, Backup and Recovery Procedures, and Supplier Security Guidelines. The ToolKit must help to map these documents directly to the applicable ISO controls and operational roles, which will be traceable and practical.

Templates should be incorporated in the fourth layer and they standardize routine compliance activities. These can be risk assessment templates, incident reporting templates, access request templates, audit checklists, and training attendance records. The AI support must allow automatic filling of repetitive fields and contextual suggestions on the basis of organizational data.

The fifth layer must be concerned with registers and inventories, which are the indicators of the continued compliance and control functioning. These are the Risk Register, Asset Inventory, Access Control Register, Incident Register, Supplier Register, and Training Register. These should be kept as live and constantly updated records in the ToolKit and not as files.

Forms, KPI sheets, dashboards, and performance metrics should be the last layer, which allows organizations to track the effectiveness of control and maturity of compliance. KPI sheets should be dynamically generated and updated based on ISO/IEC 27001 objectives, internal audit results, trends in incidents, and the effectiveness of risk treatment.

This hierarchical documentation framework will make compliance documentation complete, logically structured, and fully compliant with ISO/IEC 27001:2022 requirements.

**Predictive Intelligent Checklist Based on ISO/IEC 27001:2022 Clauses and Controls**

The second significant suggestion is the creation of a predictive intelligent checklist that will be the central navigation tool of the ToolKit. This checklist must be completely mapped to:

- ISO/IEC 27001:2022 clauses (Clauses 4–10)
- Annex A 93 control requirements.
- Evidence and organizational documentation.

Every item in the checklist must be designed to contain:

- The control reference or specific clause.
- A clear statement of the requirement in plain language.
- Contextual questions that determine the status of implementation.
- Mapping of required documentation.
- Required evidence mapping

The checklist must contain smart assessment questions that will not only focus on the presence of a control, but also the effectiveness of the control. The questions must be adjusted according to the size of the organization, industry, risk profile, and previous answers, with AI-based reasoning.

Every item in the checklist must enable organizations to give a compliance status, which includes:

- Compliant
- Partially Compliant
- Not Compliant
- Observation

This status-based method is very similar to internal audit and certification practices and enables organizations to promptly detect gaps and focus on corrective measures.

**AI-Driven Linkage Between Intelligent Checklist and Documentation Creation**

One of the innovations that this study suggests is the direct connection between the intelligent checklist and the AI-assisted documentation generation. The ToolKit must combine assessment and documentation into one workflow rather than considering them as two distinct processes.

In case a checklist item is indicated as either Not Compliant or Partially Compliant, the ToolKit must automatically:

- Determine the missing or poor documentation.
- Suggest appropriate document types (policy, procedure, register, template)
- Create preliminary documentation with the help of AI, in accordance with ISO standards.
- Recommend necessary evidence to prove implementation.

To illustrate, when an access-control control is reported to be partially compliant, the ToolKit must suggest the development or modification of an Access Control Policy, Access Request Form, Access Review Register, and similar evidence. The AI-generated drafts should be editable, and less manual and human-controlled.

This relationship renders compliance not a diagnostic process but a solution-oriented action-oriented process, which simplifies implementation significantly.

**Evidence Mapping and Automated Compliance Validation**

The other valuable recommendation is the inclusion of evidence mapping in the ToolKit. The ToolKit should identify the evidence required, such as records, logs, approvals, screenshots, training records, and audit reports, based on each checklist item and associated document.

The AI capabilities should assist in:

- Suggesting the appropriate evidence.
- Relating uploaded evidence to relevant controls and clauses.

- Labeling missing or outdated evidence.
- Indicating documentation and evidence discrepancies.

This will not only ensure compliance is not only on the presence of documents but also on provable and auditable implementation, which is what the certification bodies require.

**Semi-Automated Compliance Progress Tracking and Maturity Visualization**

The ToolKit should also include progress tracking and compliance dashboards that visualize compliance status at clauses, controls, and documentation layers. AI-driven analytics can identify patterns, such as recurring weaknesses or high-risk control areas.

Maturity indicators can be used to show the shift between initial and managed and optimized states, and organizations can learn their compliance journey. This assists in making informed decisions and prioritizing on improvement efforts.

**Role-Based Access and Usability Considerations**

The ToolKit must apply role-based access controls to maximize adoption and effectiveness, with various stakeholders (management, compliance teams, IT staff, auditors) being able to interact with the relevant sections only. User interfaces must be easy, user-friendly and in line with actual organizational processes.

The AI assistance must be integrated as contextual support, not as an intrusive automation, so that the ToolKit assists, but does not substitute, human judgment.

**Validation Through Real-World Deployment**

Lastly, the ToolKit must be tested with actual organizational implementations, pilot projects, and cycles of improvement. Predictive logic, documentation quality, and usability should be continuously improved based on feedback provided by users, auditors, and compliance professionals.

This makes the ToolKit viable, topical, and in line with the changing ISO/IEC 27001 standards and organizational requirements.

## 5.4. Limitations of the Study

Although this study offers important information on the application of ISO/IEC 27001:2022 with the help of an AI-based predictive documentation ToolKit, a number of limitations should be admitted.

Firstly, the study was founded on a cross-sectional survey design, which entailed the perceptions of organizational representatives at a single point in time. Even though this approach gives a visual representation of the challenges, advantages, and perceived usefulness of the ToolKit, it does not take into account the changes over time. The experience of the organizations in the implementation

of ISO/IEC 27001 and the introduction of AI-enabled ToolKit may vary, particularly when the staff is more experienced, the regulations are changed, or the priorities of the organization are shifted. Longitudinal data would provide a more comprehensive view of ToolKit effectiveness across the implementation lifecycle.

Second, the measurement methodology was more binary or limited-scale based, which restricted the depth of the information regarding maturity levels, the quality of documentation, or nuanced compliance practices. More specific measurement scales would be capable of measuring compliance, engagement, and learning outcomes achieved with the assistance of the ToolKit. Without such granularity, some of the subtleties in adoption matters or organizational learning would have been overlooked.

Third, the sampling method, a mix of purposive and snowball, may limit the extrapolation of findings. The respondents were selected carefully in organizations that had experience in the implementation of ISO/IEC 27001, but the sample may not be representative of the diversity of industries, organizational sizes, and geographic settings. Future studies would be useful with randomized and larger samples to enhance the belief in the generalizability of these findings.

Fourth, the evaluation of the AI-based ToolKit was primarily conceptual and perception-based. Rather than working with a fully deployed, operational ToolKit over a long period of time, respondents assessed its potential usefulness, predictive capabilities, and the capacity to make implementation less difficult. Despite the fact that these perceptions are highly informative, the real implementation may reveal other practical problems such as incompatibility with the existing enterprise systems, resistance to adoption by the users, or unforeseen technical limitations.

Finally, the research was limited to ISO/IEC 27001:2022, which restricts the direct extrapolation of the findings to other information security, quality, or governance frameworks. Although the principles of predictive documentation and intelligent compliance checklists may be implemented, different standards may possess their peculiarities that may affect the design of ToolKit, AI logic, or implementation plans.

However, the research provides a good foundation of knowledge regarding the way AI-based ToolKit can be used to support the ISO/IEC 27001 compliance and offers valuable recommendations to organizations, consultants, and developers.

## 5.5. Suggestions for Future Research

According to the findings and constraints of this study, several future research directions are proposed to advance the academic knowledge and practical application of AI-driven ToolKit in the implementation of ISO/IEC 27001.

Firstly, longitudinal research is required to establish the real impact of ToolKit in the long-term. Tracing organizations through the entire implementation process, including initial adoption, certification, and post-certification maintenance, would provide more specific information regarding the effectiveness of the ToolKit in simplifying the implementation process, improving compliance, and internal capability. Long-term studies could also be used to measure the development of living documentation and its capacity to support continuous improvement in response to new risks or regulatory changes.

Second, AI-based ToolKit should be subjected to real-life case studies and pilot applications to validate the conceptual results of this paper. Researchers will collaborate with organizations of various sizes, industries, and geographic locations to test the adoption, usability, and practical outcomes of ToolKit. The user interaction, system integration and effectiveness in generating compliant documentation will be monitored and provide actionable information to the developers and organizations.

Third, the study could be extended to other standards and frameworks, including ISO 42001, ISO 9001, HIPAA, PHIPPA, HITRUST, SOC 2 Type 2, NIST, NCA ECC, and SAMA frameworks. Comparative studies could examine how predictive documentation and intelligent compliance checklists can be adapted to various standards, find similarities, differences, and best practices in AI-enabled compliance.

Fourth, future studies could focus on more advanced AI-based decision support and predictive compliance analytics. To provide an example, the practical utility of the ToolKit can be enhanced further by adding AI to anticipate risks, identify anomalies, or predict compliance. Research can evaluate the impact of AI recommendations on decision-making, risk treatment prioritization, and audit outcomes in real organizational contexts.

Finally, research could be conducted on human factors and organizational change management in AI-enabled compliance adoption. The awareness of the barriers to user adoption, the effectiveness of training, and the support mechanisms of the leadership will be used to ensure that the ToolKit is not only technically effective but also successfully introduced into the organizational culture and workflows.

By adhering to these research directions, researchers and practitioners will be in a position to expand the knowledge of AI-driven compliance ToolKit, validate its practical use, and guide the development of more intelligent, user-friendly, and sustainable compliance solutions.

## 5.6. Final Remarks

The achievement of the ISO/IEC 27001:2022 compliance is a complicated process that extends beyond the understanding of the requirements of the standard. Even though organizations are more

likely to recognize the strategic and operational benefits of compliance, such as enhanced information security, increased stakeholder trust, and reduced regulatory risks, this information is not sufficient to ensure the implementation is successful. Organizations are frequently unable to initiate or sustain compliance efforts due to practical barriers, including the complexity of documentation, resource constraints, internal knowledge base, and operational requirements.

As highlighted in this paper, the challenges can be resolved through the application of AI-based predictive documentation and intelligent checklists, which are presented through a systematic ToolKit. The ToolKit reduces the perceived difficulty of implementation significantly by transforming compliance into an interactive, guided, and actionable process, as opposed to a document-intensive one. AI can be used by companies to generate compliant documentation, map evidence to ISO controls, and dynamically track progress, allowing compliance activities to be smoothly integrated into regular operations.

Moreover, the research also emphasizes the role of internal capability building. ToolKit can be used not only in document creation, but also as a learning platform, employees can learn about control requirements, documentation logic, and evidence expectations. This assists in retaining knowledge, reduced dependence on external consultants and organizational resilience particularly in cases where personnel turnover is high. By incorporating AI-based guidance into the compliance process, organizations will be able to balance between automation and human control, which will ensure efficiency and accuracy.

The ToolKit promotes standardization, traceability, and audit readiness, governance wise. Constant documentation that is revised to capture the changes in risk exposure, business processes, and regulatory requirements becomes the norm and not the exception. This dynamic approach enables informed decision-making, proactive risk management, and aligns compliance activities with organizational goals and enterprise risk management practices.

It is important to note that this research demonstrates that AI-based compliance solutions are not limited to large corporations. Small and medium-sized organizations can also find ToolKit very useful, as it breaks the cost and resource barrier that has traditionally been associated with ISO/IEC 27001 certification. ToolKit make sound information security management practices more democratic by providing structured guidance, semi-automated documentation, and intelligent checklist features.

The academic contribution of the study is that it bridges the gap between the complicated requirements of ISO/IEC 27001 and the implementation reality. It offers a theoretical and practical foundation of integrating AI in governance, risk, and compliance processes. Such lessons can inform practitioners, consultants, and developers to develop, deploy, and optimize AI-based compliance solutions that are not only technically viable but also user-friendly, sustainable, and adaptable to evolving organizational needs.

In conclusion, strategic leadership support, internal capability building, and intelligent AI-driven ToolKit are the most appropriate combination to guarantee ISO/IEC 27001:2022 compliance. The ToolKit approach offers a practical and realistic means of attaining sustainable, scalable, and realistic compliance through simplifying implementation, enhancing internal interaction, and permitting living documentation. As organizations continue to work in more complex information security environments, AI-based compliance solutions will play a critical role in bridging the gap between theory and operational excellence, and compliance will become an enabler of business value and not a procedural necessity.

# References


ISO/IEC. (2013). *Information technology - Security techniques - Information security management systems (ISO/IEC 27001:2013)*. International Organization for Standardization.

ISO/IEC. (2022a). *Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)*. International Organization for Standardization.

ISO/IEC. (2022b). *Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)*. International Organization for Standardization.

ISO. (2015). *Quality management systems - Requirements (ISO 9001:2015)*. International Organization for Standardization.

ISO/IEC. (2018). *Information technology - Service management - Part 1: Service management system requirements (ISO/IEC 20000-1:2018)*. International Organization for Standardization.

ISO. (2018). *Risk management - Guidelines (ISO 31000:2018)*. International Organization for Standardization.

ISO/IEC. (2023). *Information technology - Artificial intelligence - Management system (ISO/IEC 42001:2023)*. International Organization for Standardization.

Wanyonyi, V. W. (2019). *Information security management ToolKit for ISO/IEC 27001 standard: Case of SMEs*.

Gløersen, B. L. (2024). *Developing a cyber security documentation package for project deliveries*.

Böhme, R., & Moore, T. (2021). *The economics of cybersecurity: Understanding risks and incentives.*

Smith, J., & Tan, W. (2020). *Digital transformation and organizational information security.*

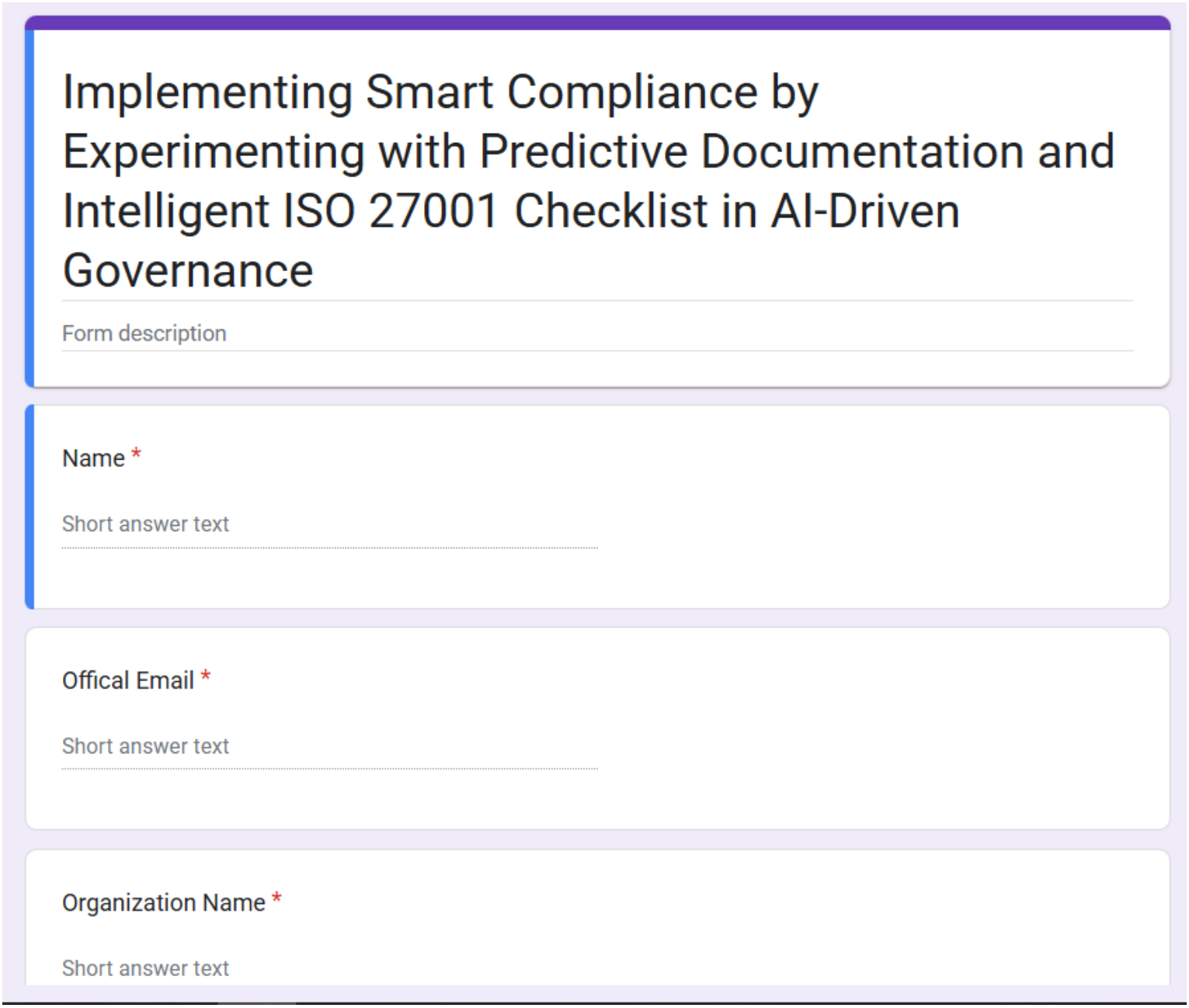
Verma, S., et al. (2019). *Information security challenges in modern enterprises.*

ENISA. (2021). *Threat landscape report 2021.*

Von Solms, R., & Von Solms, B. (2020). *Information security management principles.*

Rahman, A., et al. (2022). *AI-assisted governance tools for compliance.*

**Appendices**



Implementing Smart Compliance by Experimenting with Predictive Documentation and Intelligent ISO 27001 Checklist in AI-Driven Governance

Form description

Name *

Short answer text

Offical Email *

Short answer text

Organization Name *

Short answer text

Designation / Job Role *

- ○ Chief Executive Officer
- ○ Chief Information Security Officer
- ○ GRC Professionals
- ○ Information Security Managers
- ○ Compliance Manager
- ○ Internal Auditors
- ○ Other: .....

Years of Experience in Information Security / IT / Compliance *

- ○ Less than 1 year
- ○ 1–3 years
- ○ 3–5 years
- ○ More than 5 years

What are the main benefits of following ISO/IEC 27001 standards? *

- [ ] Improved information security
- [ ] Enhanced reputation and customer trust
- [ ] Competitive advantage in the market
- [ ] Increased customer confidence
- [ ] Improved internal processes and controls
- [ ] Compliance with legal and regulatory requirements
- [ ] Reduced chances of cyber incidents
- [ ] Other: .....

What difficulties do organizations commonly face during ISO/IEC 27001 implementation? *

- [ ] Lack of budget
- [ ] Limited skilled resources
- [ ] Technical challenges
- [ ] Heavy documentation workload
- [ ] Difficulty maintaining continuous compliance
- [ ] Understanding control requirements
- [ ] High external audit and certification cost
- [ ] Other: .....

Why do some organizations still avoid ISO/IEC 27001 certification despite its benefits? *

- [ ] High cost of certification
- [ ] Belief that existing controls are enough
- [ ] Limited knowledge or awareness of ISO 27001
- [ ] Fear of complex documentation
- [ ] Shortage of trained staff
- [ ] No requirement from clients or regulators
- [ ] Implementation seen as time-consuming
- [ ] Other: .....

How does the use of a smart, semi-automated documentation toolkit and intelligent checklist affect ISO/IEC 27001:2022 compliance in your organization? *

- [ ] Improves accuracy of compliance documentation
- [ ] Saves time and increases efficiency
- [ ] Reduces cost associated with manual processes
- [ ] Enhances internal engagement and collaboration
- [ ] Simplifies preparation for audits
- [ ] Helps identify gaps more effectively
- [ ] Other: .....

# 12% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

## Filtered from the Report

- Bibliography

## Match Groups

- 185 Not Cited or Quoted 12%
  Matches with neither in-text citation nor quotation marks
- 2 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

## Top Sources

7% Internet sources
6% Publications
10% Submitted works (Student Papers)

## Integrity Flags

**0 Integrity Flags for Review**

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Bahria University
Islamabad Campus

RC-04

MBA

## 1st Half Semester Progress Report

| | |
|---|---|
| Name of Student(s) | Ali Afzal |
| Enrollment No. | 01-321242-004 |
| Thesis/Project Title | Implementing Smart compliance by experimenting with predictive Documentation & Intelligent ISO 27001 checklist in AI Driven Governance |

**Supervisor Student Meeting Record**

| No. | Date | Place of Meeting | Topic Discussed | Signature of Student |
|---|---|---|---|---|
| 1 | 10/7/25 | Maam office | chapter 1 of thesis | Ali Afzal |
| 2 | 1/8/25 | Maam office | chapter 2 of thesis | Ali Afzal |
| 3 | 17/8/25 | Maam office | chapter 3 of thesis | Ali Afzal |
| 4 | 2/9/25 | Maam office | chapter 4 of thesis | Ali Afzal |

Progress Satisfactory [✓] Progress Unsatisfactory [ ]

Remarks: Intelligent student

Signature of Supervisor: _____ Date: 3/9/25

Name: Zahra Saleem Note:

**Students attach 1st & 2nd half progress report at the end of spiral copy.**

Bahria University
Islamabad Campus

RC-04

MBA

## 2nd Half Semester Progress Report & Thesis Approval Statement

| | |
|---|---|
| Name of Student(s) | Ali Afzal |
| Enrollment No. | 01-321242-004 |
| Thesis/Project Title | Implementing Smart Compliance by experimenting with predictive Documentation & Intelligent ESG Tool checklist in AZ Digital Governance |

**Supervisor Student Meeting Record**

| No. | Date | Place of Meeting | Topic Discussed | Signature of Student |
|---|---|---|---|---|
| 5 | 6/10/25 | Maam office | Chapter 5 of thesis | Ali Afzal |
| 6 | 12/11/25 | Maam office | Conceptual framework Amendments | Ali Afzal |
| 7 | 12/12/25 | Maam office | Conclusion of thesis | Ali Afzal |

## APPROVAL FOR EXAMINATION

Candidates' Name: Ali Afzal Enrollment No: 01-321242-004

Project/Thesis Title: Implementing smart compliance by experimenting with predictive Documentation & Intelligent ESG tool checklist in AZ Digital Governance

I hereby certify that the above candidates' thesis/project has been completed to my satisfaction and, to my belief, its standard appropriate for submission for examination. I have also conducted plagiarism test of this thesis using HEC prescribed software and found similarity index at _____ that is within the permissible limit set by the HEC for thesis/ project BBA/MBA. I have also found the thesis/project in a format recognized by the department of Business Studies.

Signature of Supervisor: _____ Date: 12/12/25

Name: Zahra Saleem