

UNIVERSITI TEKNOLOGI MARA

**UNDERSTANDING ACCOUNTING
INFORMATION SYSTEM USERS'
DILEMMAS TOWARDS INTERNAL
CONTROL GOVERNANCE: CASE
OF MULTI-SUBSIDIARY
COMPANIES**

**SUZIEL NCHAMAOBARI
OBARIEEH EPOLLO**

MSc

August 2026

UNIVERSITI TEKNOLOGI MARA

**UNDERSTANDING ACCOUNTING
INFORMATION SYSTEM USERS'
DILEMMAS TOWARDS INTERNAL
CONTROL GOVERNANCE: CASE
OF MULTI-SUBSIDIARY
COMPANIES**

SUZIEL NCHAMAOBARI OBARIEEH EPOLLO

Thesis submitted in fulfilment
of the requirements for the degree of
**Master of Science
(Accountancy)**

Faculty of Accountancy

August 2026

CONFIRMATION BY PANEL OF EXAMINERS

I certify that a Panel of Examiners has met on 7th November 2025 to conduct the final examination of Suziel Nchamaobari Obarieeh Epollo on her Master of Science thesis entitled “Understanding Accounting Information System Users’ Dilemmas Towards Internal Control Governance: Case of Multi-Subsidiary Companies” in accordance with Universiti Teknologi MARA Act 1976 (Akta 173). The Panel of Examiners recommends that the student be awarded the relevant degree. The Panel of Examiners was as follows:

Nadiah Abd Hamid, PhD
Professor
Faculty of Accountancy
Universiti Teknologi MARA
(Chairman)

Sharina Tajul Urus, PhD
Associate Professor
Faculty of Accountancy
Universiti Teknologi MARA
(Internal Examiner)

Mohamad Hisyam Selamat, PhD
Professor
Faculty of Business, Accounting and Management
SEGi University
(External Examiner)

PROF DR HJH ZURAEDA IBRAHIM
Dean
Institute of Postgraduate Studies
Universiti Teknologi MARA

Date: 7 August 2026

AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Postgraduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student : Suziel Nchamaobari Obarieeh Epollo

Student ID. No. : 2021256918

Programme : Master of Science (Accountancy) – AC750

Faculty : Faculty of Accountancy

Thesis Title : Understanding Accounting Information System Users' Dilemmas Towards Internal Control Governance: Case of Multi-Subsidiary Companies

Signature of Student :

Date : August 2026

ABSTRACT

Accounting Information Systems (AIS) are central to modern organisational operations, it serves as a critical tool to support decision-making in business planning, reporting, and operational control. Within complex multi-subsidary organisations, corporate governance (CG) as a system of rules, it establishes policies, procedures to regulate an organisation activity. Internal Control Governance (ICG), as a component of CG, governs user access, system security, compliance requirements in view of safeguarding data integrity and organisational accountability. This study explores how AIS users experience and manage dilemmas arising from ICG practices, seeking a balance particularly when control requirements conflict with operational efficiency. Adopting a qualitative research design which involves semi-structured interviews with personnel from finance, human resources (HR), and information technology (IT) departments in two multinational multi-subsidary organisations. Thematic analysis is used to indicate recurring patterns in areas where users experience difficulties while executing daily responsibilities in conformity to ICG procedures. The findings reveal key ICG related dilemmas such as regulatory compliance pressure, cybersecurity monitoring restrictions, high security system pressure, bureaucratic procedures from segregation of duties and technology-related performance anxiety. Although, ICG frameworks remain essential in ensuring authentication, mitigating system vulnerabilities, preventing data misuse, integrity and preserving informational accuracy, they also introduce operational delays, increased workload pressure, and heightened user stress. This study contributes theoretically by recontextualizing ICG in AIS as a behavioural and operational phenomenon rather than a purely technical or compliance mechanism, highlighting how governance is experienced and interpreted by users in practice. Empirically, it provides qualitative evidence on how specific ICG practices embedded in AIS create persistent dilemmas that influence user decision making, workload performance and system use within multinational subsidiary organisations. Practically, the study proposes actionable insights for organisations to design and implement ICG structures that balance control requirements with operational efficiency, reducing unnecessary workload pressure without compromising governance integrity.

ACKNOWLEDGEMENT

First and foremost, I offer my deepest gratitude and unreserved thanks to Almighty God, the Father of all creation, whose boundless grace, mercy, wisdom, and guidance have sustained me throughout this journey. From the challenging days of the COVID-19 pandemic in 2020, when this research first began, to the successful completion of this study, His unfailing strength and countless blessings have carried me through every obstacle. Every challenge and setback encountered along the way has strengthened my resolve, deepened my faith, and contributed to my personal and academic growth.

I am profoundly grateful to my family for their unwavering love, patience, encouragement, and constant support throughout my studies. My heartfelt appreciation goes to my beloved daughter, Chassey Cha-Epouruobari, my God given lovely husband, Dr. Epollo, for his words of wisdom, inspirational and enthusiastic counsel which has been my pillar and springboard for improvement and search for higher knowledge.

A special accolade to my supervisors, Dr. Noraizah Binti Abu Bakar, and Dr. Nor Hafizah Binti Abd Mansor, for their invaluable guidance, patience, and unwavering support. My appreciation also goes to Dr. Mohammad Azmi Bin Nias Ahmad (PhD, Edith Cowan University, Australia) for his constructive insights during the proposal stage.

I am profoundly grateful to Madam Dayang Rubayah Binti Awang Bohan and Madam Lulu Anak Jonathan for their continuous mentorship, as well as Professor Dr. Corina Anak Joseph, Associate Professor at the Faculty of Accountancy, UiTM Samarahan, whose critical review provided clarity and strengthened the foundation of this research.

I also extend my appreciation to all organizations that provided me with professional opportunities (employments), which has enriched my practical knowledge, broadened my expertise and strengthened my focus in this research. Special thanks to my current employer Portek and parent institution, UiTM, for availing me the platform to transcend challenges, deepened my resilience in pursuing and achieve both academic and professional career excellence.

Finally, I acknowledge that this journey, marked by trials and triumphs, has been transformative. Each barrier became a stepping stone, each challenge a lesson, and each success a testament to perseverance. This work stands not only as an academic achievement but also as a reflection of growth, resilience, and faith.

TABLE OF CONTENTS

	Page
CONFIRMATION BY PANEL OF EXAMINERS	ii
AUTHOR’S DECLARATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENT	v
TABLE OF CONTENTS	vi
LIST OF TABLES	xi
LIST OF FIGURES	xiii
LIST OF ABBREVIATIONS	xiv
CHAPTER 1 INTRODUCTION	1
1.1 Preamble	1
1.2 Background of the Study	2
1.3 Problem Statement	4
1.4 Research Objectives	5
1.5 Research Question	5
1.6 Scope of the Study	6
1.7 Significance of Study	6
1.8 Chapter Summary	7
CHAPTER 2 LITERATURE REVIEW	8
2.1 Introduction	8
2.2 Accounting Information System (AIS)	8
2.2.1 Accounting Information System (AIS) Components	9
2.2.2 Accounting Information System (AIS) and Governance	12
2.3 Internal Control Governance (ICG)	14
2.3.1 Internal Control Governance (ICG) in AIS	16
2.3.2 Internal Control Governance (ICG) Mechanism in AIS	17
2.3.3 Internal Control Governance (ICG) Practices in AIS	20
2.3.4 Internal Control Governance (ICG) Frameworks in AIS	23
2.4 Users’ Dilemmas in ICG in AIS	25
2.4.1 Accounting Information System (AIS) User’s Dilemma	26

2.4.2	Mitigating AIS User's Dilemma	30
2.5	Theoretical Foundations	32
2.5.1	Trade-Off Theory	33
2.5.2	COBIT Control Framework	35
2.5.3	Integration Theory Apply for This Study	37
2.6	Research Framework	38
2.7	Chapter Summary	40
CHAPTER 3	RESEARCH METHODOLOGY	42
3.1	Introduction	42
3.2	Philosophical Assumptions	42
3.3	Research Approach: Qualitative Approach	45
3.4	Research Technique	46
3.4.1	Case Study Approach	47
3.4.2	Data Collection Method	47
3.4.3	Case Study Selection	51
3.4.4	Data Analysis Approach	54
3.5	Reliability, Validity and Saturation	59
3.6	Research Ethics Approval	60
3.7	Chapter Summary	61
CHAPTER 4	CASE STUDY OF COMPANY A	63
4.1	Introduction	63
4.2	Background of Company A	63
4.3	Organizational and Informant Context of Company A	65
4.3.1	Organizational Structure	66
4.3.2	Demographic Profile of AIS Users in Company A	66
4.3.3	Gender Distribution	67
4.4	Summary of Data Sources for Company A	68
4.4.1	Interview Informant Codes	68
4.4.2	Department, Role and Job Scope Classification	69
4.4.3	Document Source Codes	70
4.5	ICG Practices in AIS of Company A	71
4.6	ICG Practices Creating AIS User Dilemmas of Company A	75
4.6.1	Vulnerability and IP Protection Controls	75

4.6.2	Access Authentication Requirements	76
4.6.3	Automated Audit Trail Enforcement	78
4.6.4	Alignment With Core Organizational Values	79
4.7	Dilemmas Experienced by AIS Users in Relation to ICG Practices of Company A	81
4.7.1	Regulatory Compliance Pressure	82
4.7.2	Cybersecurity Control Restriction	82
4.7.3	High Security System Pressure	83
4.7.4	Bureaucratic Procedures From Segregation of Duties	84
4.7.5	Technology-Related Performance Anxiety	84
4.8	Mitigating AIS Users' Dilemmas Related to ICG Practices of Company A	86
4.8.1	Regulatory Awareness	86
4.8.2	Procedural Compliance	87
4.8.3	Corporate Culture Alignment	88
4.8.4	Reporting Discipline	89
4.8.5	Productivity and Performance Adaptation	90
4.9	Chapter Summary	91
CHAPTER 5 CASE STUDY OF COMPANY B		93
5.1	Introduction	93
5.2	Background of Company B	93
5.3	Organizational and Informant Context of Company B	94
5.3.1	Organizational Structure	95
5.3.2	Demographic Profile of AIS Users	95
5.3.3	Gender Distribution	96
5.4	Summary of Data Sources for Company B	97
5.4.1	Interview Informant Codes	98
5.4.2	Department, Role, and Job Scope Classification	98
5.4.3	Document Source Codes	99
5.5	ICG Practices in AIS Users of Company B	100
5.6	ICG Practices Creating AIS User Dilemmas of Company B	104
5.6.1	Vulnerability and IP Protection Controls	104
5.6.2	Access Authentication Requirements	105
5.6.3	Automated Audit Trail Enforcement	106
5.6.4	Alignment With Core Organizational Values	107
5.7	Dilemmas Experienced by AIS Users in Relation to ICG Practices of Company	

B	108
5.7.1 Regulatory Compliance Pressure	109
5.7.2 Cybersecurity Control Restriction	109
5.7.3 Ethical Tension	110
5.7.4 Bureaucratic Procedures from Segregation of Duties	112
5.7.5 Technology-Related Performance Anxiety	112
5.8 Mitigating AIS User Dilemmas Related to ICG of Company B	114
5.8.1 Regulatory Awareness	115
5.8.2 Procedural Compliance	115
5.8.3 Corporate Culture Alignment	115
5.8.4 Reporting Discipline	117
5.8.5 Productivity and Performance Adaptation	117
5.9 Chapter Summary	119
 CHAPTER 6 FINDING AND DISCUSSION	 120
6.1 Introduction	120
6.2 Overview of Cross Case Analytical Approach	120
6.3 Cross Case Analysis by Research Objectives	122
6.3.1 RO1: ICG Practices Embedded in AIS That Create Dilemmas for Users	122
6.3.2 RO2: User's Dilemma Towards ICG Practices Embedded in AIS	125
6.3.3 RO3: Strategies for Balancing ICG Practices While Mitigating Operational Efficiency in AIS	128
6.4 Theoretical Interpretation Using Trade Off Theory and COBIT Framework	130
6.5 Cross Case Synthesis and Discussion	131
6.6 Chapter Summary	136
 CHAPTER 7 CONCLUSION	 137
7.1 Introduction	137
7.2 Summary of Key Findings	137
7.3 Contribution of the Study	138
7.4 Implications of the Study	142
7.5 Limitations of the Study	142
7.6 Recommendations for Future Research	143
7.7 Conclusion Remark	144

REFERENCES	145
APPENDICES	170
AUTHOR'S PROFILE	173

LIST OF TABLES

Tables	Title	Page
Table 3.1	Documentary Sources Reviewed for Data Collection	48
Table 3.2	Interview Modes by Organisation	49
Table 3.3	Thematic Analysis and Process	57
Table 4.1	Informant Demographics of Company A	67
Table 4.2	Gender of the Interview	68
Table 4.3	Interview Informant Codes of Company A	69
Table 4.4	Department, Role and Job Scope Classification	70
Table 4.5	Document Source Codes of Company A	70
Table 4.6	Department, Role and Job Scope Classification	73
Table 4.7	Summary on the ICG Practices and Resulting Dilemmas of Company A	80
Table 4.8	Summary of Dilemmas Experience by AIS User in Relation to ICG Practices of Company A	85
Table 4.9	Summary on Mitigating AIS Users' Dilemmas Related to ICG Practices of Company A	91
Table 5.1	Informant Context of Company B	94
Table 5.2	Demographic Profile of AIS Users in Company B	95
Table 5.3	Informant Demographics of Company B	96
Table 5.4	Gender of the Interviewees of Company B	97
Table 5.5	Interview Informant Codes of Company B	98

Table 5.6	Department, Role and Job Scope Classification of Company B	99
Table 5.7	Document Source Codes of Company B	99
Table 5.8	Department, Role and Job Scope Classification	102
Table 5.9	Summary of ICG Practices Creating Dilemmas for AIS Users in Company B	108
Table 5.10	Summary of Dilemmas Experienced by AIS Users in Relation to ICG Practices of Company B	113
Table 5.11	Summary on Mitigating AIS User Dilemmas Related to ICG of Company B	118
Table 6.1	RO1: Cross-Case Triangulation of ICG Practices Creating AIS User Dilemmas	123
Table 6.2	RO2: Cross-Case Triangulation of AIS User Dilemmas	126
Table 6.3	RO3: Triangulation of Mitigation Strategies Across Cases	129
Table 6.4	Cross-Case Analysis and Trade-off Patterns Across RO1–RO3	133
Table 7.1	AIS User Dilemmas, ICG Practices, Impact, and Balancing Strategies	141

LIST OF FIGURES

Figures	Title	Page
Figure 2.1	AIS Primary Component	10
Figure 2.2	COBIT Governance Framework	35
Figure 2.3	Research Framework Linking Internal Control Governance (ICG) and AIS User Experience	39
Figure 4.1	Organization Group Structure of Company A	64
Figure 4.2	Organization Chart of Company A	65
Figure 5.1	Organization Group Structure of Company B	94
Figure 5.2	Organization Group Structure of Company B	95
Figure 6.1	Cross-Case Synthesis Based on Empirical Findings	135

LIST OF ABBREVIATIONS

Abbreviations

AIS	Accounting Information System
CAS	Computerized Accounting System
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CG	Corporate Governance
CI	Code Interpretation
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COBIT	Control Objectives for Information and Related Technology
DCA	Document Company A
DCB	Document Company B
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
GRC	Governance, Risk management, and Compliance
HoD	Head of Department
HR	Human Resource
ICA	Informant Company A
ICB	Informant Company B
ICG	Internal Control Governance
ICT	Information and Communication Technology

ISACA	Information Systems Audit and Control Association
IT	Information Technology
KPI	Key Performance Indicator
LMW	Licensed Manufacturing Warehouse
LR	Literature Review
PDPA	Personal Data Protection Act
SLR	Systematic Literature Review
SME	Small and Medium Enterprise
SoD	Segregation of Duties
SOP	Standard Operating Procedure
SSM	Companies Commission of Malaysia
VPC	Virtual Private Cloud
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION

1.1 Preamble

The secret of any successful organization's financial forecasting relies on a balanced and well-structured accounting information system (AIS) control framework. This framework integrates several governance mechanisms including corporate governance (CG), corporate policy, information technology (IT) governance, and internal control governance (ICG). These mechanisms establish operational policies, strategies, internal control policies that safeguard data integrity and protect confidential information from threats such as intellectual property (IP) theft (Tombolo et al., 2023). Strong governance structures are therefore essential to ensuring data privacy, supporting compliance, and maintaining organizational accountability.

The increasing complexity of financial operations has necessitated the implementation of robust internal controls systems to ensure the accuracy and reliability of financial data (COSO, 2017; Li et al., 2023). These controls enhance accountability, mitigate fraudulent activities, and promote compliance with regulatory and statutory requirements (Al-Sahrawi, 2022; Widyaningrum, 2022). Effective internal controls strengthen the reliability of financial reporting, help prevent misconduct, and promote ethical conduct throughout an organisation (Agbejule & Nikitina, 2022). As regulatory requirements for internal control become more complex, AIS technologies have similarly advanced offering enhanced features that facilitate compliance and oversight (Soudani, 2022). Although, these expanded functionalities promote organizational oversight, they may also introduce operational inefficiencies for AIS users when system features are poorly aligned with user requirements or organizational objectives (Boateng et al., 2023).

Most modern organizations have made substantial investments in AIS or computerized accounting system (CAS) in response to addressing the complexity and time-consuming nature of managing large-scale of business activities. These systems are designed to accomplish a purposeful and goal-oriented outcome that align with overall objectives of the organization. Effective CG plays a critical role in overseeing operational activities across departments and ensuring alignment with strategic goals.

These departments typically include internal audit, compliance, finance, human resource (HR), IT, legal, risk management, business units, the executive teams, and the board of directors.

Organization policies are centred on promoting efficiency, data security and information used in daily operations. Circumventing established internal control measures in an organization constitutes a serious violation, often equated with fraud, and may lead to disciplinary action or legal consequences. AIS users working under strict deadline may experience significant stress when internal control malfunction, such as during server outages or technical glitches, which prevent essential tasks from being completed. These breakdowns directly hinder performance and disrupt financial reporting workflows during severe offline. It is informative to recognize that ICG is the core responsibility within the scope of IT governance in any organization. The reliability of financial reporting is heavily dependent on the data retrieved from the AIS. Any disruption in system functionality during critical reporting periods can significantly impair efficient productivity. In such situation, users face the choice of two unavoidable options (dilemmas) when attempting to report financial information outside the confines of AIS, which serves as the primary repository for historical data.

Internal control policies facilitate and strictly define the boundaries of how financial data may be reported including the permissible scope, prescribe format, and authorized destinations. Unauthorized disclosure or transmission of financial information without formal approval constitutes a breach of the organization's internal control regulations. The confidentiality of data and vital information's in an organization are considered highly private and restricted by rules. AIS users are prohibited from sharing internal information externally, as such actions are deemed by the CG authorities as exposure of company to external vulnerabilities.

1.2 Background of the Study

AIS refers to a structured system that collects, stores, processes, and reports financial information using both manual and computerized methods, designed to complement good decision-making and internal control activities (Romney & Steinbart, 2023). Modern AIS integrates financial reporting, internal controls, cybersecurity, and safeguards automated workflows that enhance accuracy and compliance across organizations (Saleh et al., 2023). The complexity of CG arises from the evolving ways

organizations develop and enforce internal policies that govern financial reporting and operational processes (Al-Haddad et al., 2023). This study aligns with literature in examining the balance between internal control policies and operational efficiency within organization (Haislip et al., 2023).

Organizations may struggle to remain competitive if business activities are not strategically integrated with IT functions such as information management, data analytics, and infrastructure development (De Haes et al., 2022). Well-structured IT governance advances employee engagement and contributes to improved organizational performance and profitability (Tallon et al., 2023). A well-tailored IT governance framework function as a backbone to operational efficiency and strengthen ethical management practices across organizational (Wilkin & Chenhall, 2024). An accurate financial reporting is sacrosanct for good internal decision-making and external accountability, forming the foundation of transparent governance structures (IFAC, 2023). Unwavering financial statements are essential for informing stakeholders, including investors and shareholders, in contributing to the overall transparency, trustworthiness of the organization's status and future direction.

ICG functions as a hybrid concept that integrates strategic processes and control mechanisms while interacting with complex organizational policies (Abdullah & Said, 2023). ICG serves as dominant influence in determining how organizations deploy AIS through various interrelated policies. ICG continues to evolve to enhance user effectiveness and optimize organizational resources without undermining external regulatory (Salleh & Wahab, 2023). These policies govern not only how tasks are executed but also the conditions under which they are performed while ensuring data security and privacy (Muda et al., 2023). However, as these governance policies become more complex, AIS users including accountants and finance personnel face increasingly demanding and time-consuming processes due to expanding internal control requirements (Othman et al., 2023). As a result, AIS users often experience dilemmas as they balance compliance with internal controls against the need for operational efficiency (Sholihin & Pike, 2022).

A dilemma is defined as a circumstance in which a decision-maker faces two or more competing courses of action, each producing desirable and undesirable consequences (Thiel et al., 2022; Craft, 2023). In the context of ICG, dilemmas occur when governance expectations conflict with users' operational needs, resulting in tension between compliance, efficiency, ethical responsibility, and personal judgement.

Thus, user's dilemma simplifies that an individual is at a crossroad of indecision where ethical issues infringe on universal human rights and this relates to ethical and process dilemmas mostly. Abdelraheem et al. (2021) emphasize that AIS-generated financial information must maintain accuracy, credibility, objectivity, and integrity regardless of organizational context, a standard buttress in recent AIS literature (Alduais, 2023). These qualities are essential in fostering trust in ICG, as it underpin the fundamental role it plays as the governing body of an organization (Martinez & Zhao, 2020).

1.3 Problem Statement

Every organization implements policies, rules, and regulations designed to optimize performance while ensuring the security of data and information against potential breaches and intellectual property theft. With the aim of protecting and enhancing workforce capacity, these norms are embedded within the organization's ICG framework. In practice, ICG procedures often involve multi-level authentication protocols, such as access controls, virtual private network (VPN) connectivity, and additional verification layers designed to secure financial information (Sari et al., 2022).

Nevertheless, the increasing complexity of multi-level authentication systems may create operational inefficiencies by slowing down data entry and reducing user productivity, which prior studies have identified as a barrier to effective AIS utilization (Sholihin et al., 2023). This reveals how authentication-related burdens contribute to user dilemmas within ICG in AIS. While these security protocols are critical for safeguarding data, their intricacy can place additional burdens on AIS users, who must also manage routine and demanding operational responsibilities. This complexity presents a dilemma for users, one that stems not only from technological constraints but also from the design and implementation of ICG policies themselves.

As regulatory requirements become increasingly complex, AIS users such as accountants and finance professionals are required to comply with extensive internal control procedures that can be time-consuming and cognitively demanding (Sánchez-Pérez & García-Morales, 2022). This complexity highlights a gap in understanding how regulatory pressures influence user stress, decision-making, and compliance behaviours. AIS users often face dilemmas between adhering fully to internal control protocols or by passing them to meet operational deadlines, a tension noted in recent qualitative AIS studies (Alduais, 2023). Despite these findings, limited research has

explored the ethical decision-making pressures that arise from such conflicting expectations.

This study seeks to understand the nature of user's dilemmas by exploring how user's dilemma in AIS is shaped through the implementation of ICG. AIS users bear the responsibility of upholding ethical standards while navigating rigid control mechanisms, which may create conflicts between compliance and performance expectations (Marques & Araujo, 2022). Therefore, this study examines what specific ICG practices embedded in AIS that create dilemmas for users, what dilemmas influence AIS users' decision-making and workload performance and how can these mechanisms balance the ICG requirements while mitigating operational efficiency in AIS environments. The findings are expected to provide meaningful insights for improving ICG structures and aligning them more effectively with AIS operations. By understanding the user's dilemma, it is hope that organisations can balance it operational efficiency with security and compliance expectations with ICG requirements for deadlines, particularly in departments subject to stringent reporting schedules.

1.4 Research Objectives

The main objective of this study is to understand AIS user's dilemma towards internal control governance (ICG). To achieve this main objective, the study focuses on the following specific objectives.

- a) To identify ICG practices embedded in AIS that create dilemmas for users.
- b) To identify user's dilemma towards ICG practices embedded in AIS.
- c) To explore the strategies for balancing ICG practices while mitigating operational efficiency in AIS environments.

1.5 Research Question

The main research question focuses on how AIS user's dilemma is shaped through the ICG practices. In answering the main research questions in a broader context, the following research questions were formulated:

- (i) What ICG practices embedded in AIS create dilemmas for users?

- (ii) What is the user's dilemma in ICG practices embedded in AIS?
- (iii) How can strategies balance the ICG practices while mitigating operational efficiency in AIS environments?

1.6 Scope of the Study

This study focuses on the dilemmas experienced by AIS users as a result of ICG practices implemented within organizational settings. The study is narrowed to organizations that utilize a centralised AIS alongside with established ICG practices and frameworks. Specifically in work-based context of ICG practices that shape the dilemma, pressure, and behavioural responses within AIS environment. Hence, the scope focused on the identifying the ICG practices embedded in AIS that create user's dilemma, identifying user's dilemma in AIS towards ICG practices and exploring strategies to mitigate user's dilemma in the ICG practices.

1.7 Significance of Study

This study provides valuable insights into the dilemmas experienced by AIS users within ICG environments. As organizations strengthen their governance structures, AIS users often come across conflicting expectations, operational pressures, and ethical responsibilities. Understanding these dilemmas is central due to its tendency to influence decision-making, professional judgment, and user performance.

From a theoretical standpoint, the study contributes by analysing real-time practical occurrences and user observation through the lens of relevant theories that are trade off theory and COBIT control framework. This approach deepens understanding of how dilemmas emerge in ICG settings and how they shape user experiences. By proposing a framework that acknowledges the trade-offs organizations and AIS users must navigate when balancing governance requirements, technological demands, and performance expectations. From a methodological perspective, this study used interpretivist qualitative approach that demonstrates how thematic analysis contributes to uncover complex processes, tensions, and behaviours of the AIS users that are not easily captured by conventional quantitative methods.

From a practical and industry perspective, the findings highlight the noteworthiness of incorporating flexibility within ICG to achieve a balance between

maintaining strong governance, ensuring operational efficiency, and supporting user performance. By identifying the dilemmas AIS users face, understanding why they arise, and examining how users deal with them, the study offers actionable insights that can guide organizations in refining governance approaches and improving ethical and effective decision-making. In terms of its contribution to the body of knowledge, this study integrates theoretical insights with practical occurrences to address core challenges related to AIS user dilemmas within ICG environments.

1.8 Chapter Summary

This chapter has provided an overview of the study and established the foundation for this research. It began by presenting the background of the study, outlining the increasing complexity of ICG and their implications for AIS users. The introduction highlighted how expanding governance requirements, technological developments, and organisational expectations contribute to user dilemmas, thereby framing the relevance and urgency of the study. The chapter then articulated the problem statement, by identifying the gaps in existing literature. To address these gaps, the research objectives and research questions were refined to align with the qualitative and interpretivist intent of the study. The objectives focus on identifying the types of ICG that create dilemmas, understanding why these dilemmas arise, and exploring how users deal with them in daily work practices.

The scope of this study was contextualised within the premise of AIS user dilemma within an organisation, the implementation of diverse ICG structure and CG rules to clarify the boundaries of this research. The significance of the study was also expounded, by highlighting the theoretical, methodological, practical, and industry-related contributions. These include enhancing understanding of user dilemmas through real-time hands-on experiences, proposing a model derived from qualitative findings, and offering in-depth understanding for balancing control requirements with operational efficiency. Overall, this chapter establishes the conceptual and practical notability of this research and prepares the groundwork for the Literature Review (LR) presented in Chapter Two.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews and synthesises the extant literature relevant to Accounting Information Systems (AIS), Internal Control Governance (ICG), and the dilemmas experienced by AIS users when operating within Internal Control Governance (ICG) environments. The purpose of this chapter is to establish the conceptual, theoretical, and empirical foundations to align-with the research objectives and research questions of the study. The layout for chapter two is organised into four main sections that are; Accounting Information (AIS), the following section is on the Internal control governance (ICG), further discussion on the ICG in AIS in this section. The following section discussed on the user's dilemma or issues in ICG in AIS and the last section discussed on the theoretical stances used for this study.

2.2 Accounting Information System (AIS)

Rapid technological advancements and escalating information security threats have positioned AIS as a critical component of modern organisational infrastructure. These developments have widened operational gaps that organisations must address to support current business practices, enhance decision-making processes, and manage core functions such as receivables, payables, and cash flow (Li & Chen, 2022). Integrating AIS within broader IT systems enables organisations to better manage financial and economic challenges and utilise accounting data strategically in line with technological change. Small and medium-sized enterprises in particular, depend on reliable, timely information to remain competitive in volatile markets (Romney et al., 2021). Continued investment in AIS capabilities, employee training, and process improvements strengthens organisational resilience in dynamic environments (Kumar & Tan, 2022). Such innovation contributes to improved corporate performance, reduced financial constraints, and greater access to capital markets (Smith & Lee, 2021).

Romney et al. (2021) emphasise that,

“One basic function of an AIS is to provide information useful for decision-making. With the aim to be useful, the information must be reliable, which means: (a)

it provides an accurate, complete, and timely picture of the organization's activities, (b) it is available when needed, and (c) the information and the system that produces it is protected from loss, compromise, and theft.”

Similarly, Al-Hashimy et al. (2024) state that trustworthy AIS information must present an accurate, comprehensive, and timely representation of organisational activities while ensuring the protection of both the data and the systems that generate it. AIS facilitates the detection, collection, storage, management, and delivery of accounting information as an integral component of organisational processes. Through these mechanisms, organisations can communicate effectively with internal and external stakeholders, safeguard assets, monitor employee actions, and utilise investor capital efficiently to achieve profitability and build investor confidence (Li & Chen, 2022). Martinez and Lopez (2021) highlight the ethical implications of evolving AIS technologies, noting that,

“yesterday's AIS were relatively limited observers, recorders, and reporters of data. Due to rapid advances in technology, today's AIS are powerful and far-reaching, and create opportunities for individuals who design, implement, and interact with them to cause harm intentionally or unintentionally to individuals, organizations, and societies.”

This observation emphasises the ethical responsibility of professionals and organisations to ensure that AIS innovations support rather than compromise societal and organisational well-being. Financial reports and accounting information generated through AIS must therefore meet the highest standards of accuracy, objectivity, reliability, and integrity regardless of the operational context (Ali & Noor, 2022). When effectively governed, AIS strengthens the credibility of corporate governance by reinforcing organisational values and cultivating trust, thereby enhancing opportunities for cooperation across other components of AIS and broader governance structures.

2.2.1 Accounting Information System (AIS) Components

An AIS is a structured system designed to collect, record, store, process and communicate financial and non-financial information for decision-making, control, and reporting purposes (Romney et al., 2021). As illustrated in Figure 2.1, the core components of an AIS typically include people, procedures, data, software, information technology infrastructure, and internal controls (Fontinelle, 2021). Collectively, these

components ensure that information is generated efficiently and reliably for a wide range of stakeholders, including managers, investors, and regulatory bodies. AIS functionality extends beyond technical operations to encompass ethical, operational and governance responsibilities. Because AIS influences activities such as procurement, investment evaluation, contractor engagement and human resource decisions, the information it produces is inherently connected to broader corporate governance structures

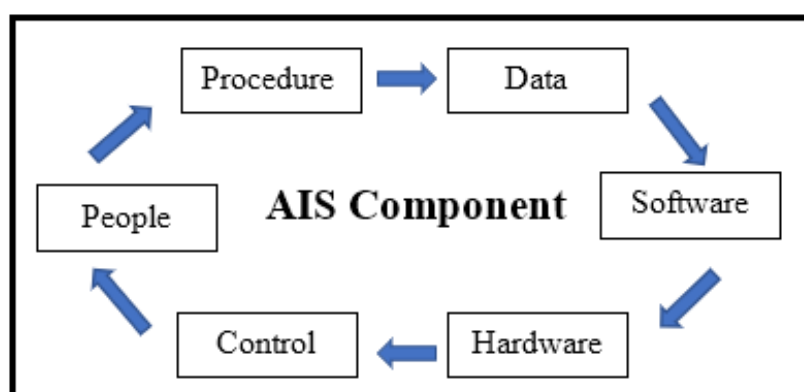


Figure 2.1 AIS Primary Component
Source: Introduction to AIS (Fontinelle, 2021)

In the context of this study, AIS components are examined through the lens of governance where complexity, decentralisation, and diverse operational environments intensify users' dilemmas (Ghazali et al., 2024). This study recognises that governance is embedded across all AIS components, shaping how users interact with, interpret, and respond to system requirements (Brandler, 2024; Li & Chen, 2022).

The *people* component includes accountants, managers, IT personnel, and auditors across different subsidiaries. In multi-subsidiary settings, AIS users often face dilemmas arising from conflicting expectations between headquarters and subsidiary-level management, differences in expertise, and varying interpretations of internal control requirements. (Ghazali et al., 2024). These challenges may affect compliance, judgement, and decision-making behaviour (Ghazali et al., 2024).

The *procedures* component, in this study, is conceptualised as organisational policies and Internal Control Governance (ICG) mechanisms. These include standard operating procedures, reporting guidelines, approval hierarchies, and compliance frameworks imposed across subsidiaries. While such policies aim to standardise operations and strengthen governance, they may also create practical dilemmas for users

when rigid controls conflict with local operational realities, time constraints, or resource limitations. In multi-subsidiary contexts, procedural governance may further intensify role dependency and approval bottlenecks (e.g., segregation of duties), creating tension between procedural compliance and operational efficiency (Wang & Zhang, 2023).

The **data** component represents both financial and non-financial information generated across subsidiaries. Users may encounter dilemmas related to data accuracy, completeness, and consistency, especially when integrating data from multiple entities with different systems or practices. Tensions may arise between the need for timely reporting and the requirement for high-quality, verifiable data under strict governance standards (Romney et al., 2021).

The **software** component includes accounting systems and enterprise platforms used across the organisation. In multi-subsidiary environments, differences in system implementation, levels of automation, or system limitations may create user dilemmas, particularly when system controls do not align with actual workflows or when users must override or bypass system constraints to meet reporting deadlines or operational needs. As governance features such as audit trails, automated approvals, and system-enforced access restrictions increase visibility and traceability, users may experience additional pressure to avoid errors and non-compliant actions (Ahmad Zazili et al., 2024; Ghazali et al., 2024).

The information technology infrastructure (**hardware** and network systems) supports the functioning of AIS across geographically dispersed subsidiaries. Variations in technological capability between subsidiaries may introduce inconsistencies in system access, processing speed, and data security, contributing to user challenges in complying with centralised internal control requirements (Li & Chen, 2022). Infrastructure constraints (e.g., unstable connectivity, limited system capacity, downtime during peak reporting periods) may also trigger dilemmas when users must choose between waiting for system restoration or finding alternative ways to complete time-critical tasks while remaining compliant (Li & Chen, 2022).

The **control** functions within AIS facilitate the implementation of management directives by providing the rules and procedures that regulate organisational conduct and reduce exposure to operational and financial risks.

According to Brandler (2024), *“Internal rules are created by the organization, executives and managers to guide internal conduct, inform customers, clients or donors and to demonstrate their compliance with external rules.”*

These controls include segregation of duties (SoD), asset protection, performance evaluations, verifications, authorisations, and reconciliations (Wang & Zhang, 2023). Accounting control specifically refers to the policies and procedures established to mitigate financial risks and ensure that reported financial information accurately reflects an organisation's economic position and performance (Li et al., 2023; Tucci, 2021). Effective control requires consistent application by both management and employees. This consistency ensures that the internal control system functions as intended while maintaining sufficient flexibility to avoid unnecessary procedural delays (Li & Chen, 2022). Risk analysis is central to this process. For example, if an organisation identifies cash theft as a primary risk, it may implement measures such as assigning one employee to each cash drawer per shift to strengthen accountability (Gordon, 2022). Similarly, within AIS environments, system-based internal controls must restrict access to authorised users and prevent unauthorised access to sensitive files and data (Dunkelberger, 2022).

Accordingly, this study places emphasis on the governance-related design and use of AIS components particularly procedures and internal controls because these mechanisms shape how users manage compliance demands while sustaining operational performance in multi-subsidiary settings (Brandler, 2024; Ghazali et al., 2024).

Overall, the definition, components and functionality of AIS demonstrate that it is not merely a technical system but a governance-dependent organisational mechanism. Its effectiveness relies heavily on well-designed internal controls, which are essential for ensuring reliability, accountability, and compliance across all AIS-related processes.

2.2.2 Accounting Information System (AIS) and Governance

AIS plays a vital role in organisational governance by supporting internal control processes, ensuring regulatory compliance, and strengthening the reliability of financial information used for decision-making. Internal control systems within AIS consist of structured policies and mechanisms designed to safeguard financial data, protect organisational assets, minimise fraud risks and support adherence to legal and regulatory requirements (Romney et al., 2021). These systems help organisations achieve strategic and operational objectives by reducing errors and mismanagement while promoting efficiency and accountability.

“Governance and internal control, although conceptually distinct, are fundamentally interconnected and often overlap in practice. Effective governance establishes the overarching framework, strategic guidance, and accountability structures that inform the design and operation of internal control systems.” (Garcia & Lee 2024)

Key elements of internal control in AIS environments include:

- (a) **Segregation of duties:** This principle involves allocating various stages of a financial transaction to separate individuals to minimize opportunities for error or fraud. Dividing responsibilities related to authorization, recording, processing, and reconciliation allows organizations to detect and mitigate irregularities more effectively (Brown & Adams, 2020).
- (b) **Physical controls:** These controls safeguard assets and sensitive information from unauthorized access, theft, or damage. Examples include restricted facility access, surveillance mechanisms and controlled entry to areas containing critical hardware or financial records (Zhang et al., 2020).
- (c) **Document controls:** These procedures ensure the security, accuracy, and integrity of financial documentation. These processes encompass the organized handling of document creation, approval, storage, and retrieval, aiming to prevent unauthorized alterations or loss (Ismail & Zainuddin, 2020).
- (d) **Information system controls:** - These controls protect digital financial data by maintaining system accuracy and preventing unauthorized access through authentication protocols, system monitoring, and secure data processing practices (Romney et al., 2021).

Collectively, these controls strengthen organisational governance by ensuring that AIS outputs are dependable, secure, and compliant with regulatory expectations. An effective AIS therefore enhances both financial reporting quality and operational accountability.

The contribution of AIS to governance is further reinforced through its alignment with established internal control frameworks, particularly the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework. Widely recognised as the global benchmark for internal control, the COSO framework outlines five interconnected components: the control environment, risk assessment, control activities, information and communication, and monitoring (Kirkpatrick, 2019). The control environment establishes the organisational culture, ethical standards and

governance principles that shape employee behaviour and guide operational practices. A strong control environment enhances compliance with regulatory and industry standards and reduces exposure to legal or reputational risks (Martinez & Clark, 2022).

Risk assessment, embedded within enterprise risk management (ERM), acknowledges that risk is inherent in organisational activities. AIS supports ERM by enabling the identification, analysis and mitigation of risks that may threaten organisational performance (Li et al., 2020). Effective risk assessment is complemented by control activities, which operationalise governance expectations by ensuring that processes are executed in accordance with prescribed procedures (Kirkpatrick, 2019). Information and communication processes also play a critical governance role by ensuring that relevant, timely and accurate information is disseminated internally and externally to meet regulatory, ethical, and operational requirements. Compliance with legal obligations and industry norms is strengthened when communication flows are consistent, documented and aligned with organisational policies (Martinez & Clark, 2022). Monitoring mechanisms further reinforce governance by evaluating the effectiveness of internal controls. Internal auditors regularly assess adherence to approved procedures, while external auditors validate compliance with regulatory and financial reporting standards. Their assessments are communicated to senior management and the board of directors, enhancing transparency and supporting oversight responsibilities (Garcia & Lee, 2021).

Overall, AIS functions not only as a technological tool but as a governance enabler. Through its integration with internal control frameworks, auditing processes and organisational risk management practices, AIS strengthens accountability, supports regulatory compliance, and ensures that organisational activities remain aligned with governance expectations. Building on this understanding, the following section examines how internal control and AIS governance operate in an integrated manner to support effective governance.

2.3 Internal Control Governance (ICG)

ICG represents a critical component of CG, as it provides the structures, responsibilities, and processes through which organisations ensure the reliability of operations, compliance, and reporting. CG broadly refers to the practices exercised by boards of directors and senior management to provide strategic direction and ensure that

organisational objectives are achieved in an accountable and transparent manner (Poppy et al., 2024). ICG supports this purpose by establishing the mechanisms that enable organisations to identify, assess, and respond to risks, safeguard assets, and maintain the integrity of financial and operational processes.

Fahmida, (2025), confirmed that *“without strong governance, internal control measures may fail to align with organizational objectives, resulting in deficiencies in risk management, operational inefficiencies, and diminished confidence in the reliability of information. Thus, robust governance is essential to ensure that internal control systems operate cohesively and effectively manage the organization’s critical risks.”*

Within this broader governance framework, internal controls are defined as the policies, procedures, and organisational structures designed to provide reasonable assurance that business objectives will be met and that undesired events can be prevented, detected, or corrected (Kirkpatrick, 2019). Effective ICG therefore ensures that control mechanisms are meticulously designed, implemented, and monitored, linking day-to-day control activities to broader organisational oversight. Although ICG is distinct from IT governance, the two intersect within AIS environments. As AIS increasingly rely on digital platforms, organisations often implement IT-related governance structures to ensure that technology supports organisational objectives and that IT-related risks are effectively managed (ISO 38500; Aminzade, 2021). In this context, IT controls become an extension of ICG, particularly where system reliability, data confidentiality, and information integrity are essential for accurate financial reporting.

Control objectives within IT-enabled AIS environments specify the desired outcomes achieved through the implementation of control procedures in specific IT activities. These objectives help regulate both system operations and user behaviour, ensuring that AIS processes remain aligned with the organisation’s ICG and its overarching corporate governance framework (Mahanti, 2021; Thomas, 2019). ICG is a foundational element of CG and within AIS environments it relies on both traditional control mechanisms and IT-related controls to ensure organisational accountability, compliance, and effective risk management. This interdependence between internal control structures and the technological capability of AIS provides the basis for understanding how AIS functions within organisations, thereby framing the discussion presented in the next section.

2.3.1 Internal Control Governance (ICG) in AIS

ICG represents the practical manifestation of corporate governance within the operational environment. It functions through policies, guidelines, and procedures that organisations establish to maintain ethical conduct, safeguard data integrity and reinforce accountability. Gordon (2022) explains that an effective ICG structure allows organisations to implement systematic compliance mechanisms, including information management protocols, risk assessment frameworks, audit functions, and performance monitoring structures. These mechanisms support alignment with governance expectations while protecting organisational data and ensuring responsibility in system utilisation. Within Accounting Information Systems, ICG typically requires the development of detailed policies that define user roles, responsibilities, and authority boundaries. Fontinelle (2021) emphasises that clarity in procedural guidelines is central to preventing misuse and ensuring consistency in data processing. Ahmad Zazili et al. (2024) further identify that ICG within AIS commonly includes access control, transaction monitoring and reconciliation procedures that maintain data reliability and protect financial information.

Kingsley and Alfred (2020) observe that internal control governance in AIS is strengthened through internal audits and continuous monitoring, which allow early identification of weaknesses or non-compliance. Ahmad et al. (2021) notes that the core purpose of ICG is to enhance operational effectiveness while protecting organisational assets and reducing the possibility of fraud. This aligns with more recent scholarship showing that control structure design in public sector AIS contributes significantly to transparency, accountability, and risk mitigation (Ahmad Zazili et al., 2024). Tucci (2021) adds that disciplined internal control processes are integral to sustaining corporate value and social responsibility. Despite these benefits, the interaction between governance requirements and system use can generate dilemmas for AIS users, particularly when compliance requirements interfere with performance expectations.

A prominent dilemma arises when organisations attempt to enforce strong control structures while simultaneously expecting prominent levels of efficiency and productivity from AIS users. Although Sulaiman and Baharudin (2021) acknowledge the complexity of balancing control and usability, they do not frame this tension as a user dilemma. In this study, the conflict is conceptualised as a dilemma because users must navigate opposing demands. On one side, stringent control are essential to protect

data accuracy, reduce fraud risk and create confidence in financial reporting outputs (Poppy et al., 2024; Turki Hazzaa et al., 2022). On the other side, heavy control layers may contribute to bureaucratic workload, slow processing time, and restrict user autonomy, resulting in operational inefficiencies and decision delays (Kamarulzaman & Ramli, 2022; Zahari et al., 2023). Organisations therefore face the challenge of maintaining strong controls without undermining workflow efficiency. Many allocate considerable resources to this balance, evaluating whether heightened security and compliance justify potential reductions in flexibility and speed. Recent findings reinforce that the sustainability of AIS governance depends on achieving equilibrium between protection and agility (Mahmud et al., 2021; Ghazali et al., 2024).

The effectiveness of ICG in AIS is influenced by its design, implementation, and ongoing supervision. Continuous assessment is required to maintain relevance, particularly in dynamic digital environments, yet such evaluations can be resource intensive (Riyadi & Setiawan, 2023). AIS users often engage directly in decisions concerning time allocation for audits, monitoring, and reporting, and this can intensify workload pressures. While strong controls protect data and uphold accountability, they may simultaneously limit decision speed or constrain employee discretion, contributing to operational tension and reduced user productivity (Ahmad Zazili et al., 2024; Zahari et al., 2023). These complexities underscore how ICG within AIS can become a source of user dilemmas, which this research seeks to explore in greater analytical depth.

2.3.2 Internal Control Governance (ICG) Mechanism in AIS

When ICG is embedded in AIS simply refers to the set of governance and control components designed, configured, and enforced within financial information systems to safeguard data, maintain accountability, and ensure regulatory conformance. These components operate as the structural foundations through which organisations achieve accuracy, traceability, and accountability in digital financial processes. Recent research shows that modern AIS environments in CG features such as role-based access control, automated approval routing, workflow authorisation, activity logging, exception reporting, and SoD-based segregation models to regulate user actions and minimise the risk of fraud or unauthorised manipulation (Rahman et al., 2023; Khalid & Othman, 2024).

Role-based access control is identified as a core ICG feature as it restricts system functions to authorised personnel and reduces opportunities for override or misuse. Similarly, audit trails embedded within AIS generate systematic logs of transactions, allowing retrospective examination and transparent accountability when irregularities arise. Studies indicate that AIS with traceable record architecture increases organisational reporting integrity and strengthens user practice compliance (Adewale et al., 2022; Widjaya & Harsono, 2024).

SoD further reinforces ICG in AIS, ensuring that no single user controls an entire financial process. However, LR expose the premise that can also lead to operational strain when task boundaries limit user capability, resulting in work delays or workflow rigidity. Abdul Wahid and Feroz (2023) are of the view that excessive segregation rules reduce user autonomy, generate system bottlenecks, and heighten emotional discomfort particularly in cases requiring urgent decisions or cross-functional processing. Exemptional reporting and automated approval escalations have been similarly recognised as dual-purpose controls, strengthening compliance yet simultaneously increasing procedural overhead and stress for system users (Yap et al., 2024).

These embedded ICG features are therefore central to understanding AIS user experience and dilemma formation, as they function not only as safeguards but also as points of operational tension where compliance and efficiency collide. This establishes the basis for the subsequent section, which examines ‘HOW’ these ICG elements interact with user decision-making, influence perception, and shape the patterns of challenge experienced in the day-to-day use of AIS. The next section (2.4) extends this discussion by analysing the nature and dimensions of AIS users’ dilemmas arising from these embedded ICG structures. Taken together, the features embedded within ICG reveal that governance controls in AIS are not merely technical safeguards but lived operational realities that shape how users think, respond, negotiate access, and perform under compliance expectations. This fluctuating balance between control and work execution creates the foundation for understanding where and why dilemmas emerge in user experience, positioning the next section to identify and classify the types of dilemmas that arise under ICG.

The integration of AIS with internal control mechanisms is fundamental to the governance of modern organisations. Internal control sets the organisation’s rules, approval processes, and accountability mechanisms, while AIS implements these

controls through automated data processing, recording, and reporting functions (Kumar & Tan, 2023). As digitalisation accelerates, internal control effectiveness is increasingly dependent on the accuracy, security, and functionality of AIS, particularly in environments that require continuous monitoring and timely decision making (Wang & Zhang, 2023).

Recent studies emphasise that internal controls embedded within AIS serve two major purposes which are regulatory assurance and operational support. Through features such as user authentication, audit trails, recorded approvals, transaction verification and real time reporting capability, the system safeguards financial information and restricts unauthorised manipulation of data (Noor et al., 2024). These embedded control procedures reinforce compliance obligations and assist organisations in fulfilling governance expectations related to transparency, accountability, and reporting credibility. In practice, AIS translates written internal control policies into enforceable digital processes that guide user actions throughout the operation cycle.

Although AIS strengthens control implementation, it can simultaneously introduce dilemmas for system users. Rigid control settings may reduce flexibility, prolong processing time, and increase the number of procedural steps required to complete routine tasks (Brown & Adams, 2023). When approval hierarchies, reconciliations or system checks are triggered frequently, users may perceive the controls as restrictive and burdensome. This tension is apparent when operational efficiency and compliance requirements do not align, leaving AIS users caught between fulfilling productivity expectations and adhering strictly to internal control rules (Martinez & Clark, 2024). Situations where policies change faster than system training further amplify this dilemma, particularly when users are held responsible for compliance failures that arise from system complexity.

Integration also reshapes how organisations manage risk. AIS supports continuous auditing, anomaly notification, transaction monitoring, and fraud detection, which enable management to identify irregularities promptly (Garcia & Lee, 2024). However, the same visibility may increase employee surveillance concerns, especially in roles where minor mistakes are automatically recorded and reported. Research indicates that increased oversight influences user confidence, decision-making behaviour, and the willingness to exercise judgment, particularly when there is concern about the repercussions of non-compliance (Hassan & Omar, 2023; Zhang et al., 2024).

Consequently, the integration of AIS and internal controls should be evaluated not only from a technical perspective but also from a behavioural standpoint.

According to Ghazali et al., (2024), *“both AIS and ICG are essential for ensuring the accuracy, reliability, and integrity of financial information while protecting stakeholder interests. AIS facilitates the systematic recording and reporting of financial transactions, providing the tools and processes necessary for accurate financial data management. In parallel, ICG establishes the structural framework for evaluating and ensuring the effectiveness of internal control mechanisms.”*

In conclusion, AIS and internal control operate as interconnected pillars of organisational governance. Their integration enhances data reliability, supports regulatory compliance, strengthens reporting integrity, and improves risk management effectiveness. Nevertheless, the interaction between these two mechanisms may also generate dilemmas for AIS users when control enforcement limits professional judgement, reduces operational flexibility or disrupts task performance. Understanding this dual impact is essential in explaining how ICG shapes user experience and subsequently frames the core phenomenon investigated in this study. Therefore, the following section discusses ICG within AIS to further establish the conceptual foundation for examining user dilemmas and decision-making in complex work environments.

2.3.3 Internal Control Governance (ICG) Practices in AIS

ICG rests on a foundation of structured mechanisms designed to ensure reliability, compliance, and operational integrity within Accounting Information Systems. Core control principles such as authorization, documentation, SoD, and security controls collectively function to protect financial information and guide organisational decision-making. Although, these controls are widely recognised, their implementation varies across organisations, sectors and operational units, creating different experiences and expectations for AIS users.

Authorization and approval form a primary control layer in AIS. Authorization grants an individual the formal right to carry out a transaction, while approval confirms that the transaction is valid, justified, and compliant with established regulations (Huang, 2019; Li et al., 2023). A key governance expectation is that these functions should not be performed by the same person, as separation limits misuse of authority

and reduces fraud risk. Management therefore sets the parameters for what can be authorised autonomously and what requires further approval, ensuring that users remain aware of procedural obligations and decision boundaries. For example, employees may be permitted to make low-value purchases independently, but transactions beyond a threshold require higher-level review. Such layered permission structures increase accountability, yet strict approval requirements may also slow task completion or reduce user discretion, illustrating how ICG can protect as well as constrain workflow.

Documentation and reconciliation further support governance reliability. Documentation ensures that every transaction is evidenced through receipts, invoices, or system-generated records (Tucci, 2021). Reconciliation involves comparing these documents to AIS entries to verify accuracy and detect inconsistencies (Kassem & Abdelhafez, 2022). In practice, the individual processing a transaction, the person verifying it, and the approver each carry shared responsibility and liability for accuracy and procedural compliance (Nguyen & Tran, 2021). To maintain control integrity, approvals should always be documented formally and never returned to the original initiator. Failure to enforce these standards increases exposure to forgery, duplicate payments, and fraud, while post-hoc approval defeats the forward-looking purpose of pre-transaction control review.

Security controls operate as another governance dimension. They include physical safeguards, cybersecurity policies and procedural access restrictions that protect data from unauthorised use (Brandler, 2024). With the growing digitalisation of organisational records, AIS environments face heightened risk of hacking, data manipulation, and confidential information leakage. Thus, access to system functions is limited strictly to authorised personnel and supporting tools such as backup services or encrypted storage maintain data resilience (Mehra, 2024). These controls frame information as a strategic resource requiring structured protection, and while essential, restrictions on data access may hinder operational flexibility or delay information retrieval for legitimate work needs.

SoD strengthens governance integrity by ensuring that no individual controls all stages of a financial transaction (Pattanaporn et al., 2022). Recording, authorisation, and reconciliation are distributed across different users to reduce error and minimise opportunity for fraud (Zhang & Lee, 2023). The principle requires responsibility sharing, workload balancing and clear policy enforcement, preventing any single user from having unchecked influence over financial outcomes (Chen & Zhang, 2022).

However, fragmentation of roles can also generate process delays or friction when users must depend on others to complete routine tasks, again reflecting the dual effect of ICG on system coordination and user autonomy.

Various categories of AIS users experience these controls according to their role, responsibility, and decision authority:

1. **Management:** Formulates strategic direction, establishes internal control policies, and oversees compliance performance to ensure that the organisation operates within acceptable risk boundaries. Finance personnel maintain financial records, input and process transactions, and handle reporting functions, making them highly exposed to procedural constraints, approval cycles, and documentary requirements.
2. **Finance department:** Maintain financial records, input and process transactions, and handle reporting functions, making them highly exposed to procedural constraints, approval cycles, and documentary requirements.
3. **IT department:** Design, manage and enforce technical controls such as user authentication, system access rights, network security, and backup measures, ensuring that AIS infrastructure remains functional and safeguarded.
4. **External auditors:** Evaluate the sufficiency of controls, review evidence trails, test system effectiveness and issue independent assessments on compliance and reporting reliability.
5. **Regulators:** Bodies that set statutory expectations, monitor adherence, and enforce reporting standards to preserve financial transparency and governance accountability across industries.

Each user group contributes to governance outcomes, yet each also faces distinct challenges when controls restrict operational judgement or increase procedural burden. ICG principles such as authorization, documentation, security, and role separation provide essential structural safeguards for AIS reliability. At the same time, these controls can introduce practical dilemmas, particularly when procedures become overly rigid or conflict with user workflow efficiency. This balance between assurance and constraint forms the theoretical premise for evaluating how formal governance frameworks are applied in AIS environments.

2.3.4 Internal Control Governance (ICG) Frameworks in AIS

ICG frameworks serve as operational structures that organisations adopt to integrate governance elements into AIS. This application is practical and execution oriented because frameworks convert governance expectations into controls, procedures, permissions, and verification steps that regulate how users manage financial data. In this section, the focus is placed on how these frameworks function inside AIS environments, how they are implemented by organisations and how their use influences user experience. The theoretical purpose of COBIT is discussed separately in Section 2.5.2 to avoid overlap.

The COSO internal control framework remains the most frequently applied model for embedding financial governance in AIS. Its five components, namely control environment, risk assessment, control activities, information, communication, and monitoring, provide a systematic foundation for transaction validation, approval enforcement, and documentation flow (Martínez & Al-Khatib, 2024). COSO application is commonly observed through structured approval hierarchies, mandatory reconciliation cycles, and traceable documentation requirements within AIS modules. Empirical studies indicate that COSO application reduces reporting discrepancies and strengthens audit readiness through unambiguous evidence trails (Fatemi & Hasan, 2022). However, COSO implementation may increase processing time and administrative documentation, which creates workflow tension and contributes to user dilemmas when operational efficiency is required (Ghazali et al., 2024).

COBIT is also widely adopted in industry practice and is included here only in its functional application. Organisations apply COBIT to align IT governance with financial reporting requirements and to structure control maturity within AIS usage (Lee & Ibrahim, 2023). COBIT enables configuration of user access rights, monitoring of audit logs, establishment of approval routing and development of compliance dashboards (Turki Hazzaa et al., 2022). These functions strengthen accountability and reduce policy breaches through rule-based automation. Despite this advantage, COBIT deployment often requires continuous system supervision and technically capable oversight teams, which may reduce user autonomy and create pressure for individuals overseeing routine accounting processes (Zahari et al., 2023). The conceptual justification for COBIT is addressed later in Section 2.5.2 as part of the theoretical foundation of the study.

The ISO 27001 security standard has become increasingly relevant to AIS following recent growth in cloud based financial systems. ISO certification provides structured security controls including encryption, authentication protocol configuration, and recovery mechanisms for data integrity (Mehra, 2024). Organisations adopting ISO 27001 often report stronger protection against unauthorised access and more defensible audit trails due to formalised documentation procedures (Riyadi & Setiawan 2023). Despite these strengths, ISO implementation requires extensive documentation maintenance and continuous compliance monitoring, which increases procedural workload for AIS users during system updates or audit cycles.

The NIST Cybersecurity Framework is also frequently incorporated into AIS for risk management and cyber defence. NIST operationalises security through identification, protection, detection, response, and recovery functions that reinforce system resilience in the event of intrusion or data corruption (Brandler, 2024). In AIS environments, NIST-aligned monitoring controls can flag abnormal access behaviour, trigger automated security responses, and track modifications to ledger entries for post-incident review (Zubair et al., 2023). While these controls reinforce assurance and accountability, scholars highlight that continuous monitoring may also create a surveillance-like environment, increasing psychological pressure and self-censorship among AIS users who fear error detection or disciplinary repercussions. The coexistence of protection and pressure reinforces the central argument that ICG functions simultaneously as an enabler and constraint, shaping how users perceive, respond to, and navigate their daily system interactions.

Ahmad Zazili et al., (2024), confirmed that “*collectively, AIS and ICG constitute integral components of an organization’s fiscal management framework. Although they serve distinct functions, they operate in a complementary and synergistic manner, reinforcing financial accuracy, transparency, and accountability, and thereby contributing to overall organizational performance and long-term sustainability.*”

This duality of protection and pressure leads directly into the following section, which examines how ICG becomes structurally embedded within AIS and how these embedded controls influence user behaviour, autonomy, and work processes.

2.4 Users' Dilemmas in ICG in AIS

In scholarly literature, a dilemma is defined as a circumstance in which a decision-maker faces two or more competing courses of action, each producing desirable and undesirable consequences (Thiel et al., 2022; Craft, 2023). Concisely from researcher viewpoint, user's dilemma simplifies that an individual is at a crossroad of indecision where ethical issues infringe on universal human rights; this phrase typically relates to ethical and process dilemmas. In the context of ICG, dilemmas occur when governance expectations conflict with users' operational needs, resulting in tension between compliance, efficiency, ethical responsibility, and personal judgement. Recent studies emphasise that dilemmas are not merely operational interruptions, but cognitive and moral conflicts that force users to weigh accuracy, timeliness, accountability, and risk exposure simultaneously (Ghazali et al., 2024; Mahmud et al., 2023).

ICG is positioned at the heart of this conflict. The OECD (2023) describes ICG as the organisational capability to achieve objectives reliably while managing uncertainty and upholding integrity. Research shows that ICG strengthens accountability, reporting reliability, and cyber-resilience, yet simultaneously increases the likelihood of ethical and procedural conflicts during system use (Tucci, 2022; Brandler, 2024; Zubair et al., 2023). When controls are rigid, hierarchical, or technologically complex, users may experience restrictions that complicate task execution, affect decision confidence, and trigger dilemma-based behavioural responses.

The centrality of the human role in AIS intensifies these dilemmas. Although automation, AI-driven processing, and digital verification tools continue to expand, human discretion remains necessary in judgement-based tasks such as approval decisions, exception handling, and interpretation of irregular transactions (Alles & Gray, 2022; Li & Chen, 2023). AIS output is ultimately dependent on decisions made by accountants, analysts, auditors, managers, and regulators, whose ethical reasoning influences data quality and reporting credibility (Poppy et al., 2024). Thus, technological sophistication does not eliminate human responsibility; instead, it increases the weight of judgement required to navigate competing control expectations (Kumar & Patel, 2023).

Recent empirical research confirms that AIS users frequently experience pressure when performing repetitive control-intensive tasks, particularly where

approvals, documentation trails, access verification, or reconciliation are mandatory (Abdelraheem, 2023; Nguyen & Tran, 2024). Governance requirements designed to prevent fraud and ensure transparency can also extend processing time, limit autonomy, or create role dependency, producing frustration, system fatigue, or reduced task adaptability (Kassem & Abdelhafez, 2023; Rahim & Siddiqui, 2023). Users are therefore caught between complying to protect integrity and adapting to maintain workflow performance, illustrating a direct tension that forms the basis of AIS user dilemmas.

2.4.1 Accounting Information System (AIS) User's Dilemma

AIS users frequently encounter dilemmas regarding their roles and responsibilities, while CG helps drive positive results that support organizational performance and objectives. According to Tucci (2021) and the OECD (2014), CG extends beyond the administrative policies of Governance, Risk management, and Compliance (GRC) and ethics; it also holds both the organisation and its members accountable. This accountability includes the actions of all users, encompassing not only employees but also the governing bodies of institutions and the organisation (Gordon et al., 2022). The interactions between CG and AIS users are neither simple nor predictable, as structural, and operational factors influence users' dilemmas and obligatory issues that must be managed during their daily tasks (Ahmed & Noor, 2021).

High expectations set by top boards and managers motivate AIS users to rigorously follow internal controls and maintain professional ethics within their organisation (Poppy et al., 2024). This research aims to explore the dilemmas faced by AIS users in the context of ICG within organisations. Studying the dilemmas encountered by AIS users and the role of ICG helps to understand how organisations might alleviate the pressures imposed by these demanding requirements. The high structural and operational expectations often manifest as stringent rules and regulations implemented through organizational policies (Wang & Liu, 2021). These complexities contribute significantly to the dilemmas experienced by AIS users. Such factors fall within the operational standards established by the organisation's governing bodies, both internal and external. The persistent concern about identifying irregular transactions and behaviours has led to the introduction of new asset monitoring procedures and physical audits. Additional issues include managerial concerns

regarding payment schedules, repeated payments, and determining who can be trusted to approve transactions, as well as the procedures for implementing corrective actions against fraud.

The need to effectively identify errors related to ICG and AIS user practices has necessitated the enforcement of stringent rules within the organisation. Consequently, AIS users face both process and ethical dilemmas as they must navigate numerous internal controls while using AIS tools to perform their daily tasks. The workload has become increasingly burdensome because processes are deeply embedded with complex controls in AIS tools and compounded by organizational rules and regulations (Zhang & Lee, 2023). Due to these internal controls, AIS users are often compelled to work extended hours, sometimes late into the night, to complete their tasks, as each transaction is time-consuming and subject to strict deadlines. This continuous and demanding workload pressures AIS user to work beyond ethical and permissible hours, thereby risking violations of labour laws and fundamental human rights.

AIS user's dilemma generally manifests in two dominant forms that are; procedural dilemmas and ethical dilemmas. Procedural dilemmas arise when users must decide whether to adhere strictly to control protocols or adjust procedures to maintain workflow efficiency (Rahim & Siddiqui, 2023; Zazili et al., 2024). Ethical dilemmas emerge when users are torn between following governance requirements and exercising personal judgement to achieve fairness, timeliness, or organisational benefit (Craft, 2023; Hazzaa et al., 2024). Both forms reflect situations in which compliance and efficiency compete as priorities rather than operate in harmony.

- (a) **Process dilemma** - The relationship between CG and AIS users is multifaceted and frequently subject to unpredictability, influenced by diverse structural and operational challenges encountered in daily tasks (Ahmed & Noor, 2021). CG frameworks establish rigorous policies and control mechanisms that regulate how AIS users' access, process, and manage financial data. Consequently, users are required to manoeuvre through complex protocols aimed at safeguarding data security, ensuring accountability, and maintaining compliance with regulatory standards (Haniffa & Hudaib, 2020). Such operational constraints necessitate that user uphold heightened vigilance and consistently adjust to the dynamic nature of security measures and organizational policies. These dynamics often lead to procedural challenges that may impact the efficiency and effectiveness of AIS utilization.

(b) **Ethical dilemma** - This dilemma arises at the intersection where an individual faces a difficult choice due to conflicting ethical considerations, particularly when organizational policies or actions potentially infringe upon universal human rights. In the context of AIS, ethical dilemmas occur when users are required to balance the organizations' expectations concerning the deployment and utilization of AIS tools with their own moral judgements and professional integrity. AIS users and other business professionals are often required to operate within strict timeframes and performance standards, which can sometimes pressure them to compromise ethical principles for the sake of efficiency or compliance. These dilemmas highlight the tension between adhering to prescribed organizational norms and safeguarding fundamental ethical standards, such as privacy, transparency, and fairness. The complexity of these situations is further heightened by the evolving nature of technology and the varying interpretations of ethical behaviour across different organizational cultures (Alles, 2020).

On the other hand, IT personnel are responsible for educating staff about the requirements of ICG in AIS, as this area is often regarded as complex and challenging, particularly regarding issues such as access bypass, VPN connections, multi-level authentication, and verification (Romney et al., 2021). Since only a limited number of users are allowed to access an AIS module at any given time, other AIS users are prevented from accessing the same module concurrently. This necessitates that AIS users prioritise access for others, as each data entry depends on the completion of postings from a single user. Consequently, this arrangement increases the difficulty and time required to complete their work.

The more intricate the policies that are implemented, the more challenging it becomes for AIS users to navigate the strict internal control system while maintaining efficiency in their regular tasks (Kassem & Abdelhafez, 2022). AIS users must remain vigilant to ensure that all activities are conducted ethically and correctly, while simultaneously meeting demanding deadlines. Despite this, due to the operational and structural challenges encountered daily, the relationship between CG and AIS users is neither straightforward nor simple. Conflicts often emerge between the necessity for strong controls and the users' struggles to complete their daily responsibilities efficiently (Pattanaporn et al., 2022). As a result of these dilemmas, AIS users are

frequently faced with the difficult choice of either adhering strictly to rules and regulations or attempting to manipulate the system to meet their objectives.

As career professionals, AIS users often find themselves constrained by stringent demands that require them to work long hours, sometimes staying awake day and night until their tasks are completed. Despite these pressures, the justification for strong internal controls motivates AIS users to maintain their integrity and professionalism. This motivation helps shape and sharpen their skills, enabling them to achieve optimal performance if they choose to persevere (Wang & Hsieh, 2020). However, this dilemma creates a bottleneck or point of congestion between AIS users and the internal control systems in place. Failure to manage the persistent dilemmas and workload challenges may lead to increased resignation rates, which in turn disrupt organizational productivity (Rahim & Siddiqui, 2021). Therefore, this research aims to explore a suitable framework for analysing and addressing the academic gaps related to the dilemmas faced by AIS users in the context of ICG.

Previous studies indicate that the implementation of ICG within AIS frequently generates tensions that shape user experience, decision-making and work behaviour. A recurring dilemma emerges when users must balance compliance with evolving regulatory requirements while maintaining efficient system execution. Studies show that heightened policy awareness and fear of non-compliance can inhibit autonomy in system interaction, resulting in excessive caution and reduced decision speed (Lee & Rahman, 2023; Osman et al., 2024). Users are often aware that non-adherence may lead to audit triggers or governance scrutiny, creating a constant psychological tension between risk avoidance and workflow continuity.

ICG also introduces dilemmas arising from procedural obligation and process rigidity. Governance policies such as multi-layer approvals, authentication checkpoints and SoD structures are designed to strengthen accountability, yet they can restrict operational fluidity and prolong decision cycles (Karim & Fathil, 2023). Where users are expected to meet deadlines while simultaneously complying with control protocols, the conflict between procedural obedience and timely completion of tasks becomes increasingly visible.

Cultural dynamics further intensify these tensions. organizational environments that emphasize hierarchical authority and risk-averse behaviour may discourage discretionary judgement, even when system constraints hinder task completion (Hashim & Lau, 2022). Users may struggle between respecting formal governance expectations

and adapting system usage to maintain productivity, particularly where informal practices exist alongside formal policies.

Another dilemma relates to increasing expectations for transparent reporting and real-time traceability. AIS generates audit trails, error logs and documentation trails that enhance governance visibility, but these features can amplify pressure on users to always produce error-free outputs in daily tasks (Cheng & Abdullah, 2023). The expectation to maintain perfect reporting accuracy while working under time and data-volume constraints may lead to cognitive overload and occasional strategic avoidance of system- recorded decisions.

Literature highlights tensions between productivity expectations and performance metrics embedded within AIS. When governance controls slow data processing or create repetitive verification tasks, users experience stress between maintaining efficiency and remaining fully compliant (Nur & Yusoff, 2024). This clash is particularly evident in environments where output is measured quantitatively but control compliance is evaluated qualitatively, leaving users caught between speed-driven performance targets and control-driven governance requirements.

2.4.2 Mitigating AIS User's Dilemma

Ethics within organizational contexts refers to the principles that guide individual conduct, ensuring that actions align with moral values and contribute positively to the interests of stakeholders (Ahmed & Noor, 2021). Within the context of AIS, users often face a range of ethical and procedural dilemmas that directly impact their performance and decision-making. These dilemmas arise from the intersection of professional ethical standards, internal control mechanisms, and the broader governance structures that regulate financial and operational activities.

Another key area is regulatory awareness, which requires users to remain up to date with evolving compliance requirements to ensure alignment with current laws and standards (Ahmed & Noor, 2021). Additionally, AIS users must follow strict internal procedures that may not always correspond with the real time demands of operational efficiency (Haniffa & Hudaib, 2020). Nevertheless, multi-national corporate culture also contributes to these dilemmas, as organizational norms and values can either support or conflict with ethical decision-making, particularly across diverse cultural and regulatory contexts (Alles, 2020). Furthermore, AIS users experience pressure related

to productivity and performance, as they are often expected to meet high output targets despite constraints imposed by complex internal control systems (Tucci, 2021). Consequently, the requirement to comply with rigorous reporting standards, emphasizing accuracy, consistency, and transparency, places additional responsibility on AIS users to meet external expectations while upholding ethical and professional standards (Ahmed & Noor, 2021).

As dilemmas are multifaceted and interconnected as they are further complicated by the complexity of ICG structures. The technical requirements of information systems, and the organizational expectations established by corporate governance policies are all the bounding dilemmas. For example, regulatory mandates may necessitate extensive documentation and system controls, while essential for audit readiness, can hinder workflow and reduce overall productivity.

In practice, AIS users must devote considerable time and cognitive effort to navigating these challenges while maintaining compliance and upholding ethical standards. The pressure to meet performance expectations set by corporate governance authorities, boards of directors, shareholders, and external regulators further intensify the psychological and operational demands placed on users. This often results in stress, reduced efficiency, and performance fatigue, particularly in high-volume transactional environments.

To manage these conflicts effectively, users must exercise professional judgment and ethical discernment, balancing system obligations with the practical realities of organizational operations. These findings underscore the importance of designing internal control frameworks that are not only robust and compliant but also responsive to user experience and operational efficiency within AIS environments.

AIS users often face intricate challenges arising from the necessity to enforce robust control measures designed to prevent fraud and other forms of financial misconduct. These controls necessitate the integration of multiple layers of security protocols, which are designed to safeguard the integrity and confidentiality of financial data within the organisation (Alles, 2020). The layered security framework encompasses technical, procedural, and administrative safeguards, all of which must function in unison to identify, prevent, and reduce potential risks. Although, these robust controls are crucial for upholding organizational integrity and adhering to regulatory standards, they simultaneously present operational challenges for AIS users. These challenges frequently position AIS users in situations where they must reconcile

the requirements of security compliance with the need for efficiency and practicality in their daily tasks.

In summary, literature illustrates that AIS users face dilemmas that originate from regulatory expectations, procedural constraints, cultural norms, reporting visibility, and productivity demands. These dilemmas reflect structural and behavioural tensions rather than isolated incidents, revealing misalignments between governance intent and operational reality. The section is to explore the underlying conditions that cause these dilemmas to arise and intensify within ICG-regulated AIS environments.

2.5 Theoretical Foundations

The development of a theoretical foundation represents the initial and most critical stage of this research, as it guides how data will be collected, analysed, and interpreted. A robust theoretical framework ensures that the study remains grounded in established academic logic while providing direction for identifying themes, patterns and relationships embedded in the data (Kam et al., 2023). In line with this, it is necessary to identify a theory that both aligns with the research objectives and reflects the philosophical position of the study (Nguyen & Lee, 2024). This alignment allows the researcher to frame problem boundaries clearly and create conceptual coherence between literature, methodology, findings, and theoretical interpretation.

Although, this research adopts a qualitative approach, early literature review remains essential for defining the research boundary and identifying relevant constructs. Patel and Davidson (2023) emphasise that in qualitative inquiry, theoretical positioning must evolve through iterative engagement with data rather than through predetermined measurement variables. Thus, while the literature provides initial direction, theory gains meaning progressively as themes emerge from field evidence. Observation, document analysis, and interview interaction are therefore positioned as key sources of insight in this study, allowing phenomena to be understood from the perspective of AIS users directly experiencing ICG dilemmas.

Observation offers a surface-level interpretation of user behaviour, whereas interview-driven data provides depth by revealing reasoning, rationalisation, and emotion behind user actions (Vivek et al., 2024). According to Smith and Johnson (2023), preliminary theoretical propositions can guide data interrogation at the early stage of research, but the framework must expand inductively as richer empirical insight

emerges. The present research follows this approach by allowing initial theoretical understanding to guide question formulation and data exploration, while still permitting emergent findings to refine or reshape theoretical boundaries.

This study therefore adopts a theory-driven approach supported by interview transcripts, observational notes, and verification through internal documentation. Such triangulation maintains analytical neutrality and reduces interpretive bias, ensuring that meaning is derived from informants lived experiences rather than researcher assumption. In line with Creswell and Poth (2023), theoretical sensitivity is applied throughout coding and theme development to ensure that data remain the core driver of interpretation rather than pre-existing conceptual expectation. Through this process, the research establishes a clear philosophical stance and positions Trade-Off Theory as the primary theoretical anchor for understanding dilemmas faced by AIS users under ICG pressure.

This study recognises that AIS users constantly negotiate between accuracy, compliance, efficiency, and ethical obligation. The resulting tension directly reflects the logic of Trade-Off Theory, making it the most suitable foundation for explaining the behaviour, judgment and work outcomes emerging from ICG-driven environments. The following section therefore proceeds to discuss Trade-Off Theory in detail and demonstrates how its principles underpin this research.

2.5.1 Trade-Off Theory

The Trade-Off Theory in organisational research hypothesizes that decision makers must often balance competing priorities where improvement in one domain may require concession in another. These conflicts, known as trade-off dilemmas, occur when no single option can simultaneously satisfy performance, governance, and resource objectives. The theory therefore provides a foundational lens to examine how organisations make choices under constraint, particularly where risk, efficiency and control interests collide (Cui et al., 2023).

Classical roots of the theory can be traced to March and Simon, who introduced the concept of bounded rationality, arguing that individuals make decisions within limits of information, time, and cognitive capacity (March & Simon, 1958). They demonstrated that trade-offs manifest when organisations pursue efficiency yet risk losing adaptability, or when they prioritise standardisation while constraining

flexibility. Contemporary scholarship extends this work by showing how modern environments characterised by audit digitalisation, real-time reporting and cybersecurity threats intensify such tensions (Nguyen & Lee, 2024).

Within AIS settings, these trade-offs are visible where governance demands accuracy, traceability, and error prevention, while operational teams emphasise workflow speed and practical task completion. As controls increase, discretion narrows and workload expands, leading to performance strain when users must choose between strict procedural obedience and timely output delivery. Trade-Off Theory therefore becomes essential for analysing the lived realities of AIS users who operate under dual pressures of compliance and productivity.

In alignment with this study, trade-off dilemmas experienced by AIS users emerge across three interlinked dimensions:

- (i) balancing control compliance with workflow efficiency, particularly when reporting deadlines conflict with detailed verification, approval cycles, and record validation.
- (ii) maintaining system integrity through layered controls that prevent fraud and unauthorised access but simultaneously create process delays, decision bottlenecks, and reduced user autonomy.
- (iii) managing the cost–benefit relationship of control implementation, where organisational investment in security, monitoring and documentation should be justified against training burdens, system complexity, and reduced task fluidity.

Trade-Off Theory therefore provides a structured rationale for examining how AIS users negotiate these tensions and how such negotiations shape decision-making patterns, behavioural responses, and performance outcomes. By grounding this research in trade-off logic, the study is positioned to explain not only what dilemmas occur, but why they persist within environments governed by ICG expectations. Understanding trade-offs conceptually sets the foundation for identifying where governance pressures originate. To examine this relationship further, the next subsection evaluates the COBIT control framework as a reference model that institutionalises ICG practices within AIS environments and contributes directly to the emergence of user-level dilemmas.

2.5.2 COBIT Control Framework

A control framework provides a structured foundation for designing, implementing, and monitoring internal control activities within an organisation. Its purpose is to manage uncertainty through coordinated practices that promote reliability, compliance, and consistency in operational processes. Among the various models available, COBIT (Control Objectives for Information and Related Technologies) has emerged as the leading global reference for IT governance due to its comprehensive structure, strategic alignment features, and strong linkage between technology assurance and corporate accountability (ISACA, 2023).

COBIT emphasises governance through measurable objectives, maturity models and defined control processes that guide system implementation and performance evaluation. It supports organisations in aligning technology resources with business strategy, improving investment returns, and reducing information-related risks that arise from system misuse, data leakages, or unauthorised access (Aversano & Tortorella, 2023). Recent research highlights that COBIT is particularly relevant in environments with sophisticated transactional systems such as AIS, where decision-making depends heavily on information quality, processing fluidity, and audit integrity (Matar & Salah, 2024). This study therefore adopts COBIT as the structural lens for understanding how internal controls are activated, monitored, and enforced among AIS users, particularly when ICG expectations intersect with operational realities.

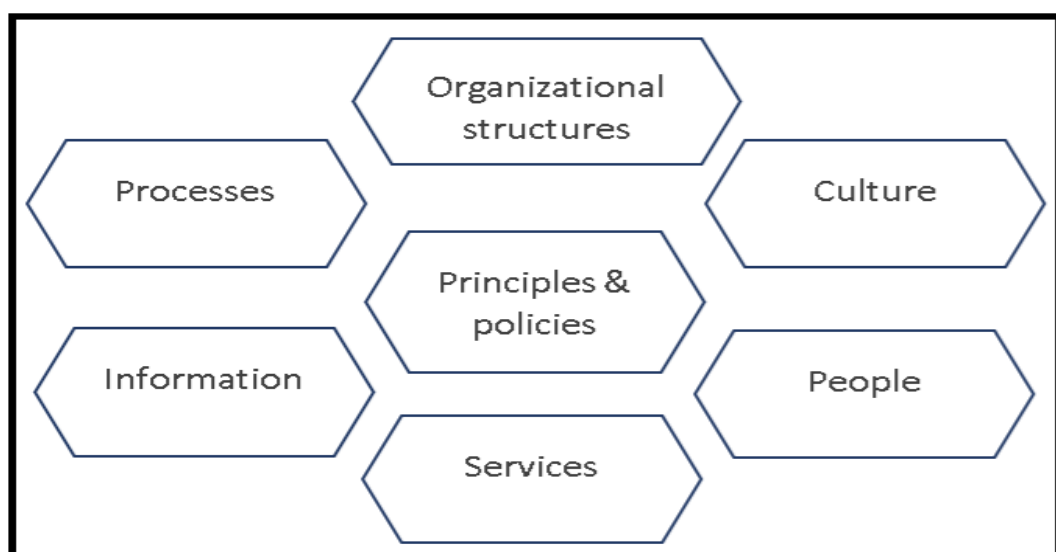


Figure 2.2 COBIT Governance Framework

Source: <https://www.audit-academy.be/en/glossary/cobit-governance-framework>

Figure 2.2 illustrates the COBIT governance architecture. It comprises several governance enablers including organisational structure, policy principles, defined processes, data management, role-specific responsibilities, service delivery mechanisms, and corporate culture. These enablers reflect the interaction between AIS users, system controls, and managerial authority. Policies and process design determine workflow boundaries, while access rights, authentication layers and systematic documentation shape user decisions, autonomy, and behavioural discretion. Through this lens, AIS personnel are positioned not merely as system operators but as governance agents whose actions generate accountability trails and influence corporate compliance outcomes.

From an internal corporate governance (ICG) standpoint, COBIT strengthens oversight by clarifying reporting channels, performance indicators, and role segregation expectations. Senior management monitors IT activities through defined metrics, while middle-level personnel execute operational controls structured around traceability, verification, and approval hierarchy. These responsibilities are embedded into system workflows, requiring AIS users to navigate authentication steps, data review processes and documentation requirements that protect audit transparency but simultaneously impose procedural tension when deadlines, workload, and compliance demand overlap (Zhang & Lee, 2023). Internal control is therefore reinforced not only as a policy artefact but as a lived operational constraint that shapes user discretion, task speed, and decision behaviour.

Internationally recognised standards such as ISO 38500 complement COBIT by defining governance of ICT as the directed and controlled use of technology through evaluation, strategic alignment, and continuous monitoring. When applied within AIS environments, governance standards intensify emphasis on fraud prevention, cyber risk mitigation, and information stewardship. As a result, system flexibility tightens and users experience increasing pressure to comply with procedural rigor, particularly where data privacy, approval escalation and SoD are enforced to safeguard organisational integrity (Zein et al., 2024). COBIT therefore provides a governance-centred architecture that explains how control expectations are embedded into AIS workflows, how user discretion is shaped by system design, and how dilemmas emerge when operational needs intersect with compliance obligations. Having established COBIT as the structural grounding for ICG-driven controls, the following section

synthesises both theoretical lenses to demonstrate how trade-offs and COBIT control frameworks use for this study.

2.5.3 Integration Theory Apply for This Study

The integration of Trade-Off Theory with the COBIT control framework establishes a structured analytical foundation for understanding how AIS users navigate organisational expectations, technological safeguards, and ethical accountability under ICG environments. The theoretical positioning developed in Sections 2.5.1 and 2.5.2 forms the basis upon which decision tensions, control burdens and behavioural responses are interpreted in later empirical chapters. Trade-Off Theory highlights the constant negotiation between efficiency, compliance, data protection, and workflow autonomy, while the COBIT framework provides a governance-oriented representation of how controls, processes and access responsibilities are formally executed within information systems (ISACA, 2023). Together, these lenses enable an assessment of how internal control mechanisms can simultaneously support and constrain user performance.

This study adopts these two theoretical pillars to explain the dynamics observed in AIS practice, where users often operate at the intersection of competing priorities. Central to this analytical structure is the understanding that internal controls do not function in isolation, but rather as interacting elements shaped by organisational rules, cybersecurity protocols, and ethical responsibilities. Recent qualitative governance scholarship indicates that AIS behaviours are influenced not only by policy design rather by the way individuals interpret risk, trust system reliability, and manage surveillance-based accountability (Rahman, 2022; Silva & Noronha, 2023). The theoretical integration applied in this study therefore examines control pressure as more than a technical artefact by positioning it as a human-centred decision environment.

The integration of Trade-Off Theory forms the theoretical foundation of the framework by recognising that organisations rarely achieve control, efficiency, and flexibility simultaneously. Internal control enforcement often requires negotiation between accuracy and timeliness, oversight and autonomy, and compliance and productivity (Nguyen & Lee, 2024). AIS environments therefore become settings where users must constantly negotiate competing expectations. In this regard, the framework positions control implementation not only as a technical function but as a behavioural

space where individuals make judgement calls, interpret policy, and respond under pressure. These tensions align with emerging governance literature, which highlights how digital compliance systems create both stability and friction in routine work (Silva & Noronha, 2023). Four core analytical dimensions guide interpretation reflecting the intersection of theory with organisational reality:

- (i) Organizational governance logic, drawn from Trade-Off Theory, which explains how management seeks efficiency, transparency and protection of financial information while simultaneously imposing restrictions that may delay workflow.
- (ii) AIS control architecture, aligned with the COBIT framework, used to evaluate how access structures, audit logs, verification protocols, and process approvals shape user accountability within financial systems.
- (iii) Cybersecurity assurance and technological constraint, which considers how authentication design, monitoring intensity and system complexity influence control compliance and error-avoidance behaviour.
- (iv) Ethical and professional judgement, where dilemmas arise in balancing policy adherence with situational pressures such as workload intensity, deadline conflict, and fairness in system decision outcomes. work processes.

2.6 Research Framework

Figure 2.3 also reflects that internal control within AIS operates as part of broader IT governance rather than as an isolated administrative requirement. ICG directives extend into system configuration, access stewardship, audit sequencing, and decision accountability, affecting not only IT departments but all operational users (Aminzade, 2021). As organisations scale and regulatory expectations intensify, the likelihood of operational tension increases, particularly where workflows involve sequential authorisation, multi-level approvals, or high-frequency transaction processing (Rahman, 2022). The framework therefore serves as a structural lens for analysing how AIS users interpret, manage, and respond to these controls during live work execution. The research framework for this study was developed through the synthesis of literature, theoretical grounding and alignment to the research objectives (RO) and research questions (RQ). The framework positions C as the policy-setting authority and Internal Control as the operational mechanism that embeds governance

principles within AIS structures. These controls subsequently shape how AIS functions and how users experience, negotiate and respond to system-regulated constraints while performing their daily roles. The study seeks to explain how ICG requirements actively shape user experience within AIS, how performance dilemmas emerge, and how trade-offs influence task decisions.

In the figure 2.3, CG is positioned at the top as the originating source of organisational policies and rules. The arrow flowing from CG to AIS indicates that governance expectations guide the development of system requirements, constraints and oversight features embedded within the AIS. Internal Control, shown on the left side of the figure, connected to AIS through an arrow that illustrates the translation of governance requirements into control procedures, such as access restrictions, approval structures, and compliance mechanisms. This emphasises that the AIS operates as a controlled environment shaped by the organisation's internal control design. The arrow from AIS-to-AIS Users indicates that user experience influenced by the system's design, including the constraints, access rights and work processes imposed on them. The operational features of AIS influence users' tasks, reporting activities, and decision-making processes.

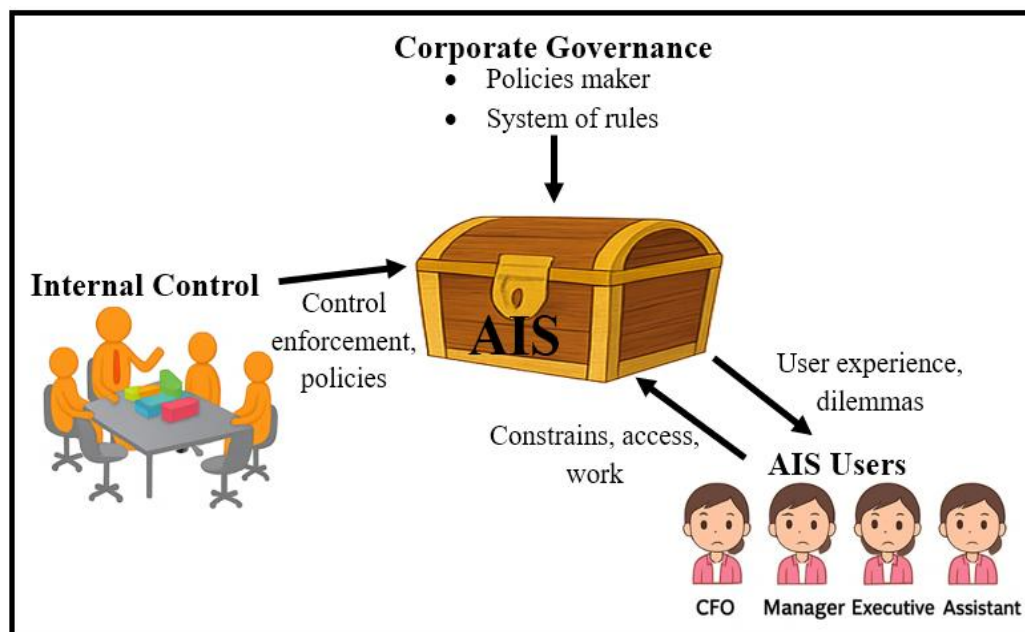


Figure 2.3 Research Framework Linking Internal Control Governance (ICG) and AIS User Experience
Source: Developed for the Current Study

Figure 2.3 above shows how governance expectations pass through internal controls to the AIS, influencing user experience. The arrows in the research framework represent the direction of influence and the sequence of interactions among CG, Internal Control, AIS, and AIS Users. This explanation clarifies how the components in the framework work together, helping readers move smoothly into later sections where these elements are connected to real-world themes. Collectively these arrows show the continuous cycle of control application and user adaptation, positioning the AIS environment as both a governance instrument and a behavioural influence zone.

2.7 Chapter Summary

This chapter has presented a comprehensive review of scholarly literature relevant to AIS, corporate governance, internal control structures, and user decision-making within technology-enabled environments. The review drew upon high-quality and recent academic sources, particularly studies published beyond 2022, to ensure that theoretical and practical insights reflected current developments in digital governance, system security, and organizational accountability. The purpose of this synthesis was to establish conceptual clarity, point to recurring issues surrounding AIS usage, and identify the mechanisms through which ICG contributes to user dilemmas in work execution.

Through examining empirical and theoretical contributions, the chapter demonstrated how internal control structures influence user autonomy, processing efficiency, and ethical conduct. Recent literature increasingly emphasizes tensions between compliance requirements and operational flexibility, showing that governance expectations may protect data integrity while simultaneously generating time pressure, workflow rigidity, and decision stress among AIS users. In reviewing these dynamics, the chapter revealed how internal control constraints extend beyond procedural compliance, affecting behavioural responses, productivity, and the quality of decision outcomes in real organizational settings.

The chapter also integrated theoretical foundations, specifically Trade-Off Theory and the COBIT governance framework, positioning them as interpretive lenses for understanding user dilemmas within digitally governed workplaces. The theoretical and structural alignments developed here form the basis of the research framework

introduced in Section 2.6, which maps the relationship between ICG factors, AIS features, workflow challenges, and user-centred outcomes. This framework directly supports the research objectives and provides an analytical pathway for subsequent data collection and interpretation.

In summary, this literature review establishes the academic grounding necessary for the empirical phase of this study. This chapter identifies knowledge gaps, points out organizational challenges, and links theory to the experiences of AIS users. It lays the groundwork for Chapter Three, which provides a detailed account of the research design, methodology, sampling strategy, ethical considerations, and data collection process.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

A well-constructed methodology forms the foundation of a rigorous scientific inquiry as it outlines the philosophical stance, research approach and structured procedures undertaken to obtain and interpret findings. According to Creswell and Poth (2023), methodology is critical as it determines how knowledge is generated, how assumptions are justified and how evidence is analysed in a transparent and replicable manner. Therefore, this chapter presents the methodological framework adopted for this research including the philosophical assumptions, research approach, case study design and procedures for data collection and analysis.

This study adopts a qualitative interpretive design, supported by semi-structured interviews and document analysis, with thematic analysis as the analytical method. The chosen approach allows deeper interpretation of AIS user experience and ICG practices within a natural organisational context, aligning with Nguyen and Lee (2024), who emphasise that qualitative research is most suitable when exploring lived realities, behavioural patterns, and contextual complexity. Such methodological positioning not only reflects the exploratory nature of the present study but also reinforces the need to engage interpretive reasoning when analysing interactions between users, systems, and governance controls. Such methodological alignment is rooted in the underlying philosophical assumptions that guide how knowledge, reality and meaning are interpreted in this research, leading into the next section.

3.2 Philosophical Assumptions

Philosophical assumptions represent the foundational belief system that directs scientific inquiry and forms the basis for qualitative research. Merriam and Tisdell (2020) explain that these assumptions inform how a study conceptualizes reality, constructs knowledge, and determines the value and role of the researcher. They are typically organized across four key domains: ontology, epistemology, axiology, and methodology. As explained by Nguyen and Lee (2024), these domains are interdependent and collectively guide the framing of research questions, selection of

research strategies, interpretation of phenomena, and construction of meaning. Ontology addresses assumptions regarding the nature of reality, epistemology concerns the origins and justification of knowledge, methodology relates to the strategies employed to study the phenomenon, while axiology focuses on the influence of values in the research process.

These philosophical assumptions collectively inform how the findings of a case study are interpreted and presented. They form the theoretical framework that guides the researcher in collecting, analysing, and interpreting the data. This framework may also draw from foundational philosophical principles such as the law of identity (associated with ontology) and the law of non-contradiction (related to epistemology), which are further simplified through ethical and aesthetic considerations (Allemang, 2022).

Merriam and Tisdell (2020) emphasized that researchers must first recognize and understand the paradigm they choose for their study, as this paradigm significantly influences how data are interpreted, how the research is designed, and how findings are ultimately communicated. Similarly, Catherine et al. (2021) described a research paradigm as a system of shared beliefs about cause and effect, necessity, and possibility that informs the metaphysical structure of a study.

Metaphysics concerns itself with the fundamental and first principles that define abstract concepts of reality and the underlying basis of worldviews. It seeks to explain the nature of existence, the structure of the world, individuals' beliefs within it, and the potential relationships among its various components. As noted by Catherine et al. (2021), shared metaphysical belief systems can serve as a guiding framework for research, influencing not only the methodological approach but also the ontological and epistemological perspectives.

Pattanaporn et al. (2022) further supported this view by emphasizing that ontology and epistemology are deeply interrelated in the context of social science, making methodological choices both significant and consequential. According to Sabri and Jumaa (2022), epistemological approaches to research can be broadly categorized into positivist, critical, and interpretive paradigms. Merriam and Tisdell (2020) also noted that the distinctions between interpretive and positivist paradigms can be better understood by examining their respective ontological and epistemological foundations, both of which are concerned with the nature of knowledge and the reality it seeks to represent.

The main premise in Pattanaporn et al. (2022) regarding positivism is that the social world exists independently of human perception and that its properties should be measured using objective, unbiased methods rather than inferred subjectively through impressions or perceptions. Lisa (2011) described positivists as those who believe that reality is separate from the individual observer. Positivists regard the subject (the researcher) and the object (the phenomena under study) as two distinct and independent entities. Their goal is to establish knowledge about a reality that exists beyond the human mind. According to Janet and David (2023), positivists maintain that human understanding reflects an objective, sovereign reality, which serves as the foundation for knowledge.

In contrast, interpretivism asserts that reality is not objective or external but is socially constructed through the meanings people assign to their experiences within the metaphysical world. Janet and David (2023) explain that the interpretive paradigm allows researchers to employ a variety of methodologies to enhance the understanding of the knowledge and the problem under investigation. Similarly, Bianchi (2023) notes that the interpretive paradigm emphasizes using methodologies that are appropriate to the research problem, free from the constraints of conflict-driven philosophical debates. Fundamentally, research situated within the interpretivist paradigm exhibits the following key characteristics:

- (i) It rejects the positivist assumption that social science methods can uncover an objective ‘truth’ about the real world.
- (ii) Positivist epistemology embraces objectivity in research, asserting that researchers must prevent their personal biases from influencing the outcomes.
- (iii) Therefore, researcher neutrality is paramount to avoid the intrusion of personal predispositions or values by systematically following established procedures from beginning to end.
- (iv) In contrast, interpretivist epistemology assumes that the researcher and the subject of inquiry are interconnected in a collaborative process, with each influencing the other.

Given these distinctions, the present research adopts an interpretivist philosophical stance. The central aim of interpretivist research is to understand how social actors construct meaning within their lived contexts. Fylan (2005) states that interpretivism enables researchers to explore subjective experiences and uncover how individuals validate and interpret their realities. Dillon (2023) affirms that this paradigm

is particularly valuable when research seeks to explain how beliefs and intentions shape behaviour. Guba and Lincoln (2005) extend this view by arguing that interpretivism uncovers the relationships between social structures, personal perceptions, and everyday practice. The interpretive philosophy is therefore highly suitable for this study, which seeks to understand the dilemmas encountered by AIS users in relation to ICG. It aligns with the exploratory nature of the research questions, which address the how, what, where, and why of user experiences. As Bianchi (2023) notes, interpretive studies are especially effective for emerging research areas where little is known about the lived experiences of participants. By adopting this approach, the study can contribute to CG and IT governance discourse by identifying the gaps in communication, misalignment of perspectives, and the challenges experienced by AIS users.

In summary, the philosophical assumptions of this research are grounded in ontology, epistemology, axiology, and methodology, framed within an interpretivist paradigm. This paradigm supports the use of flexible qualitative strategies such as privilege meaning, experience, and social interaction. It enables the study to uncover how AIS users navigate internal control dilemmas, how they interpret constraints or tensions, and how these interpretations influence system outcomes. The interpretive stance therefore provides a coherent foundation for the methodological choices that follow in subsequent sections of this chapter, particularly the adoption of a qualitative approach, which will be discussed in Section 3.3.

3.3 Research Approach: Qualitative Approach

This research employs a qualitative approach to obtain in-depth understanding of AIS user experiences and the contextual factors that shape those experiences within organizational settings (Creswell & Poth, 2023; Berkovich, 2018). Qualitative inquiry is particularly appropriate for examining how users navigate AIS under different layers of organizational control, including ICG structures and CG expectations. It enables exploration of practical occurrences, real perceptions and behavioural responses that may not be visible through quantitative measurement alone. As elaborated by Aspers and Corte (2019), qualitative methods are valuable for capturing meanings, reasoning, and personal interpretation, which aligns directly with the objectives of this study.

The research draws on purposive sampling, document review, and semi-structured interviews to generate rich empirical insights. Twenty-eight informants were

selected from two multi-national multi-subsidiary organizations, representing senior, middle and operational levels. Their involvement was not intended to produce statistical representation, but to provide sufficient narrative breadth to trace how ICG mechanisms influence AIS usage across hierarchical functions. Hennink and Kaiser (2022) noted that thematic saturation is often achieved within a modest sample when participant groups share comparable operational environments, making the number selected appropriate for a study of this scope.

Interview sessions ranged between 30 and 60 minutes, allowing participants time to articulate routine practices, constraints, and decision-making behaviours that emerge when AIS processes intersect with ICG and CG requirements. The emphasis was placed on depth of discussion rather than volume of respondents to ensure conceptual richness. This structure supports interpretive analysis, enabling the research to uncover tension, alignment and reasoning behind user actions, approval structures, error escalation, control compliance, and governance requirements.

The chosen qualitative approach therefore provides a methodological basis for the specific techniques applied in this research. The next section discusses these techniques in detail, outlining the procedures for interview execution, documentary evidence collection and the analytic framework used to extract themes representing user experience within AIS under the influence of ICG and CG structures.

3.4 Research Technique

Every research study relies on structured and methodical approaches to ensure the systematic collection, analysis, and interpretation of data. These approaches are fundamental to maintaining the integrity, validity, and reliability of the research process. By employing a clear and well-defined methodology, researcher is able to generate insights that are both meaningful and trustworthy, ultimately contributing to a comprehensive and accurate understanding of the research problem. Methodological rigor is especially important when dealing with complex research questions that require nuanced interpretation and contextual understanding.

In the context of qualitative research, methodological decisions take on added significance due to the interpretive nature of the data. Unlike quantitative research, which focuses on numerical measurement and statistical inference, qualitative research emphasizes understanding phenomena through detailed descriptions, patterns, and

themes derived from participants' experiences and perspectives. As such, the selection of an appropriate analytical method is critical to shaping the depth, richness, and credibility of the findings. The analytical method not only influences how data are examined and presented but also determines the extent to which the study can uncover underlying meanings, contextual influences, and relationships between key concepts. A carefully chosen analysis technique allows the researcher to move beyond surface-level observations to explore deeper insights, ultimately enhancing the contribution of the study to existing knowledge. Furthermore, alignment between the research objectives, data collection methods, and analytical approach ensures that the study maintains internal coherence and analytical consistency.

3.4.1 Case Study Approach

This study employs a multiple-case study approach, which is recognised as a robust qualitative strategy for examining contemporary organisational phenomena within real-life environments (Yin, 2020). Since AIS usage and ICG involve dynamic interactions between technological controls, human decision-making, and structural authority, the case study method allows context-embedded investigation rather than abstract analysis.

A multiple-case design was selected over a single-case strategy to enable comparative evaluation of AIS use and governance experiences across different organisational structures. Comparison between Company A and Company B strengthens conceptual validity, improves generalisability of findings, and helps identify recurring patterns, contrasts, or behavioural variations across environments. The case study framework directly informs the subsequent data collection techniques deployed namely document review and interviews which form the foundation of empirical evidence for this research. With the case study framework established, the following section details the data collection mechanisms that enabled information extraction from both documentary sources and organisational participants.

3.4.2 Data Collection Method

The information obtained in this research is based on real-time, first-hand accounts of events and practical experiences. Generally, this data was retrieved from both direct and indirect sources possessing comprehensive knowledge of the

occurrences and behaviours under study. Consequently, a purposive sampling strategy was employed, selecting informants based on their relevant knowledge and experience in using the AIS tool, as well as their organizational positions (Fylan, 2005; Teddlie & Yu, 2007; Tongco, 2007). Data collection involved observations and semi-structured interviews, which complemented unstructured interviews and aligned well with the overall research design. Additionally, this study incorporated document reviews alongside interviews and interview questions to provide a comprehensive context for interpreting the research findings.

3.4.2.1 Document Review

Document review was adopted as a primary method of qualitative data collection to support interview findings and to provide contextual grounding for AIS usage and ICG practices within the selected organisations. In qualitative case-based inquiry, documentary sources are treated as primary data that reflect actual policy intent, organisational structure, and governance requirements (Silverman et al., 2023). To meet the requirement for transparency and traceability, all documents utilised in this research are now clearly itemised with document names, issuing authority, year of publication and source access reference.

The documentary materials reviewed comprised operational, regulatory, and governance-related records obtained from internal management repositories, departmental archives, and controlled-access databases. A structured summary of these documents is presented in Table 3.1 below.

Table 3.1
Documentary Sources Reviewed for Data Collection

No	Type/ Title of Document	Issuing Department / Source	Year Available / Last Updated	Purpose of Use in Research
1	Business Model	Strategic Management Division	2025	To understand core activities, functional workflow, value creation, and organization environment.
2	Corporate Structure	Corporate Secretariat	2022	To identify governance hierarchy, reporting flow, and parent-subsidiary relationship.
3	Organization Charts	Human Resource Department	2024	To map job roles, reporting authority, and positioning of AIS

				users within organizational structure.
4	Financial Reports	Finance Department	2025	To examine financial reporting processes, control-checkpoints, and audit-relevant evidence trails.
5	Policies, Rules & Guidelines	Internal Governance / IT / Compliance Unit	2024	To identify internal control mechanisms, approval routing, SoD and regulatory compliance frameworks.

Source: Developed for the Current Study

3.4.2.2 Interview

The interview method adopted in this study was semi-structured, enabling open-ended discussion rather than rigid questioning based on fixed sequences. This approach allowed the researcher to probe deeper into user interpretation, behavioural responses, and operational dilemmas experienced within AIS under ICG and CG environments. Interview guides were developed based on the organisational context of informants, ensuring relevance to their job functions, system exposure, level of authority, and governance responsibilities.

Interviews were conducted using multiple communication modes to accommodate informant availability and organisational schedules. These included face-to-face sessions, phone discussions, email exchanges, online platforms such as Google Meet, Skype, and WhatsApp. The duration of each interview ranged between 30 and 60 minutes, with sessions scheduled over several months to allow reflection, clarification, and validation of responses where necessary. The interviewer used a semi-structured protocol to minimise ambiguity, provide conversational flexibility, and promote a two-way flow of inquiry, consistent with qualitative interpretive research.

A total of 28 informants were interviewed across two organisations (Company A and Company B), representing operational, managerial, and executive roles. The interview process, participant identification, session period, and mode of communication are summarised in Table 3.2 below.

Table 3.2
Interview Modes by Organisation

Interview Characteristics	Company A	Company B
Interview Period (Month/Year)	April 2023-Jan 2024	May 2023-Mar 2024
Number of Informants	14	14

Interview Duration per Session	30–60 minutes
Method of Informants Identification	AIS users with ICG responsibilities
Interview Structure	Semi-structured, open-ended, conversational
Mode / Platform Used	Face-to-face, Email, Phone, Google Meet, WhatsApp

Source: Developed for the Current Study

To support consistency across all interviews and ensure that responses were comparable between Company A and Company B, a formal interview protocol was designed. The development of this protocol and the guiding questions used during the interviews are presented in the following section.

3.4.2.3 Interview Protocol & Questions

The interview protocol for this study was designed to ensure structured data acquisition while maintaining conversational flexibility as show in Appendix A below. A semi structured interview format was selected because it enables exploratory dialogue, encourages elaboration, and allows the researcher to probe for clarification when required. This approach is widely recommended in qualitative research because it provides deeper insight into behavioural responses, organisational realities, and governance challenges experienced by AIS users (Rahman & Sulaiman 2024; Lee & Hassan 2023).

Interview questions were developed in direct alignment with the research objectives and thematic concerns identified in the literature review. Three core areas guided the construction of the questionnaire: the profile and background of informants, ICG mechanisms in AIS environments, and the dilemmas faced by users along with implications for performance. The Malay language was used during the interview sessions to ensure clarity, comfort, and natural expression. After transcription, data were translated into English for analysis and presentation in the thesis.

Prior to each interview session, participants were screened based on their job role, length of work experience, involvement with AIS and familiarity with ICG. This ensured that all responses originated from individuals with practical exposure and decision-making responsibility within the AIS environment. The protocol supported consistent execution of interviews while remaining adaptable to real time discussion dynamics.

This interview protocol ensured that all informants were guided through a logical sequence of discussion while allowing individual experiences and perspectives to emerge naturally. This interview protocol ensured that all informants were guided through a logical sequence of discussion while allowing individual experiences and perspectives to emerge naturally. Although the informants held roles across operational, middle, and senior management levels, from CEO to assistant level, the same set of interview questions was administered to all 14 informants. This approach was justified because the study aimed to capture a comprehensive understanding of ICG-related dilemmas in AIS from multiple hierarchical perspectives, rather than focusing solely on level-specific experiences. Using a uniform interview guide allowed for consistent comparison across roles, highlighting both shared and unique challenges in AIS usage while ensuring that insights could be synthesized into a coherent analysis. Level-specific nuances were captured through probing and follow-up questions tailored to each informant's experience during the semi-structured interviews.

3.4.3 Case Study Selection

Following the description of the data collection strategy, this section explains how the two case organisations and their respective informants were selected. This research adopts a dual-case study strategy involving two multinational subsidiary companies. The approach allows for cross-case comparison to evaluate whether similar ICG conditions influence AIS users in comparable or contrasting ways. Case selection plays a critical role in qualitative inquiry, as it determines the relevance, richness, and depth of information obtainable from real organisational settings. Therefore, the selection process prioritised companies that demonstrated complex operational structures, structured AIS environments, and governance mechanisms strong enough to reflect control-driven work interactions.

The use of two cases enables triangulation and strengthens analytical credibility by allowing patterns, themes, and governance dilemmas to be compared rather than observed in isolation. This ensures that findings are derived not merely from single-case characteristics but from overlapping behavioural, procedural and control mechanisms occurring across two real corporate environments.

3.4.3.1 Selection of Case Study

The selection of Company A and Company B was purposefully made based on relevance, accessibility, and alignment with the objectives of this study. In qualitative research, case selection must be justified based on the capacity of the setting to generate meaningful insights (Creswell & Poth, 2023; Tracy, 2022). Accordingly, both companies were chosen because they exhibit similar organisational characteristics that make them suitable environments for investigating AIS usage within the context of ICG.

This selection is supported by three justification criteria. The first justification relates to governance suitability. Both companies operate as multi-national multi-subsidiaries under foreign headquarters, with more than thirty-five global entities governed through centralised financial reporting systems. This reflects an important level of internal control enforcement, multi-layered approval structures, and strong dependency on ICG. These features provide an appropriate setting to observe AIS related dilemmas that emerge from compliance expectations, workflow constraints, and procedural control enforcement.

The second justification concerns comparability of AIS implementation to allow meaningful cross case analysis. Despite operating in different industries, both organisations employ enterprise level AIS or Enterprise Resource Planning (ERP) systems to support financial consolidation, transaction authorisation, data accuracy monitoring, and regulatory reporting. The similarity in technological infrastructure reduces systematic bias and enables the study to focus on variations in governance practices rather than software or system limitations.

The third justification pertains to access feasibility and richness of data. Access to key AIS users was ethically granted through professional contact with internal stakeholders. This accessibility enabled interviews with individuals personally responsible for system operation, approval execution, and control compliance. The information obtained from these informants is grounded in real practice and reflects lived operational experiences rather than surface level observations. This ensured that the dataset was sufficiently deep, reflective, and analytically meaningful.

In compliance with the Personal Data Protection Act 2010 (PDPA) and organisational privacy requirements, both companies are anonymised throughout this thesis. Internal documents were reviewed in controlled settings, and only non-sensitive

information has been retained for academic reporting. Where necessary, details have been generalised to prevent organisational identification.

As summarised in Table 3.2 (Interview Modes by Organisation), fourteen informants from each company were interviewed. Selection was based on relevance of job scope, involvement in AIS utilisation, and authority within the control governance workflow. This approach strengthens the validity of findings by ensuring that the perspectives captured are those of individuals who actively experience, manage, and navigate internal control mechanisms within AIS.

Therefore, the selected cases were not chosen arbitrarily. They were intentionally identified as the most appropriate contexts for examining AIS governance complexities, enabling this study to meaningfully explore operational dilemmas, behavioural responses, and governance consequences within real organisational environments.

3.4.3.2 Selection of Informants

The selection of informants from both participating companies was determined based on their critical roles in operating and managing AIS within an ICG environment. Key personnel such as CFOs, finance managers, tax managers, IT staff, and finance-related professionals were purposefully identified, as these individuals interact most frequently with transaction modules, approval workflows, system access rights, and audit trails. They are responsible for processing sensitive financial information, interpreting system-embedded control rules, and ensuring that operations are aligned with organisational governance expectations. The identified informants generally perform tasks that place them at the core of AIS-driven decision-making and compliance monitoring. Their responsibilities typically include but not limited to:

1. **Designing and implementing internal controls:** AIS users may be involved in the design and implementation of internal controls aimed at preventing fraud and other types of financial misconduct. Such controls often include SoD, access controls, transaction monitoring, and maintaining a backup audit trail.
2. **Ensuring compliance with laws, regulations, and internal policies:** AIS users may be responsible for ensuring that the organization's AIS complies with relevant laws, regulations, and internal policies. This responsibility may involve

reviewing the system's processes and controls to verify that they meet the required standards.

3. **Assessing and evaluating the effectiveness of internal controls:** AIS users may be involved in the ongoing assessment and evaluation of the organization's internal controls to ensure their appropriateness and effectiveness. This process may include reviewing the design and implementation of controls, evaluating their functionality, and identifying and addressing any weaknesses or deficiencies discovered.
4. **Providing support and guidance to other users of the system:** AIS users may also be responsible for providing support and guidance to other system users, assisting them in understanding, and using the AIS effectively and efficiently. Additionally, AIS users play a critical role in identifying errors, system modules, and weaknesses that require attention and improvement.

These functions position AIS users as the most suitable group to provide insight into control-related challenges, behavioural responses, system limitations, and governance dilemmas. Accordingly, the demographic distribution of informants by role and organisation will be discussed in Chapter 4 (Company A) and Chapter 5 (Company B), which outline the seniority levels and departmental placement of the informants involved in this study. Following the identification of suitable informants and the justification for their involvement, the next phase of this study concerns how the collected qualitative evidence will be interpreted and transformed into meaningful research outcomes. As this study is exploratory in nature and grounded in real organisational practices, the analytical process plays a crucial role in connecting interview narratives, observed behaviours and document findings to theoretical understanding.

3.4.4 Data Analysis Approach

All data gathered and compiled consist of information that requires careful interpretation and application of logical and analytical reasoning to identify meaningful trends, correlations, or patterns within the dataset. The process involves organizing raw data systematically and conducting a thorough examination to uncover underlying relationships among variables or recurring themes relevant to the research questions. To achieve this, the raw data will be analysed and manually coded using rigorous coding

techniques, allowing for the categorization and synthesis of qualitative information. Thematic analysis, a widely recognized qualitative data analysis method, will be employed to guide the formulation of key themes. This approach involves iterative coding, where data segments are grouped based on shared characteristics or concepts, facilitating a structured understanding of the phenomena under study. Through this manual coding process, the research aims to provide a nuanced interpretation of the data, supporting the development of robust findings and contributing to the overall validity and reliability of the study.

3.4.4.1 Thematic Analysis

Thematic analysis is recognised as a foundational interpretive method within hermeneutic qualitative inquiry. It enables the systematic identification of patterns of meaning through inductive development of themes and categories. According to Braun and Clarke (2016), thematic analysis requires immersive engagement with the dataset to identify, analyse, and interpret recurring patterns that meaningfully represent informant experiences. Recent methodological reviews affirm that thematic analysis remains relevant due to its flexibility, transparency, and suitability for complex organisational research contexts involving human behaviour, technology, and control structures (Nowell et al., 2023; Vaismoradi et al., 2022). Although, it begins descriptively, the process becomes interpretative during categorisation, clustering and meaning construction. Coding decisions require judgement, conceptual reflection, and comparison across transcripts. Table 3.3 (Thematic Analysis and Process) demonstrates the six sequential phases applied in this study. The method facilitated the identification of patterns related to AIS usage, control expectations, and user dilemmas, aligning with the study objective of interpreting lived realities through Trade Off Theory and qualitative meaning structures.

Manual coding was selected to enhance depth of interpretation, reflexive reasoning, and transparency. This approach enables the researcher to remain actively engaged with transcripts rather than relying on automated software output. Manual interpretation supports theory building by allowing meanings, contradictions, tensions, and implicit trade-offs to surface through repeated reading. Such depth is necessary in AIS related studies where compliance, control and operational behaviour intersect (Hidayat & Rahman, 2024). Thematic analysis in this study supported the development

of conceptual understanding from observed behaviours, narratives, and operational descriptions. It facilitated the interpretation of actions and decisions within ICG structures and made visible the trade-offs experienced by informants during AIS use.

This approach was particularly suitable for interpreting layered dilemmas, behavioural responses to control mechanisms and cognitive decision pathways. It revealed explicit policies as well as implicit working norms that shape AIS practice. Thematic analysis allowed the researcher to uncover how users negotiate control, efficiency, autonomy, and accountability, which aligns directly with RO1 and RO2. Due to the sensitivity of organisational information involved, thematic analysis ensured ethical handling through controlled classification, anonymisation, and abstraction. Its suitability for confidential industrial research has been supported by recent qualitative ethics discussions (Lobe et al., 2023).

Table 3.3 presents the adapted thematic analysis process, structured around Braun and Clarke (2006) and informed by recent research utilisation in organisational information systems. Appendix B consolidates code categories, extract sources, and theme interpretation, ensuring methodological clarity and auditability for replication and validation.

Table 3.3
Thematic Analysis and Process

Step	Phase	Description of Process
1	Become familiar with the data and transcribing	The first step involved familiarization with the fourteen informants from both Company A and Company B. The researcher coordinated and confirmed individual schedules through physical meetings and electronic communication platforms to arrange the interview sessions. Following this, all collected data were obtained and thoroughly reviewed to gain a comprehensive overview of the dataset. This process included interpreting and transcribing the responses from all informants by carefully reading the materials and making preliminary notes. Finally, the researcher systematically reviewed the data to identify and remove redundant or duplicate information, ensuring that only clear and usable statements were retained for further analysis.
2	Generate code	After reviewing all the transcripts, the data were systematically coded based on the researcher's interpretation. Key words and phrases were highlighted using various colour codes, each corresponding to a distinct theme or concept identified within the text. Each code represented a specific idea or event relevant to the study. At this stage, the researcher carefully examined each interview transcript, identifying and marking segments that appeared significant or potentially insightful. Relevant phrases and sentences were aligned with the established codes. Following this detailed review, all data were organized into groups defined by these codes, enabling a concise summary of key points and recurring patterns across the data from both Company A and Company B. The color-coded system facilitated efficient comparison and analysis of the findings.
3	Search for themes	Following the initial coding process, the researcher examined the generated codes to identify patterns and began developing broader themes. Themes are more abstract and encompassing than individual codes. During this phase, some codes were found to be too vague or irrelevant and were subsequently discarded. Conversely, certain codes evolved into distinct sub-themes as their significance became clearer. This iterative process involved multiple reviews of the data, with emerging insights continually informing the researcher's analytical decisions. At this stage, the researcher sought to identify potential themes that would illuminate the underlying phenomena within the dataset.
4	Review themes	Next, the researcher ensured that the identified themes accurately and comprehensively represented the data. This process involved reviewing each theme alongside its supporting data extracts to verify completeness and internal coherence. The researcher critically evaluated whether any relevant aspects had been overlooked and assessed the extent to which the themes were substantiated by empirical evidence. Based on this review, themes were refined by dividing, merging, eliminating, or

		revising them to enhance their clarity, relevance, and explanatory power. Themes that no longer aligned with the research objectives were adjusted or removed to maintain the integrity of the analysis.
5	Define themes	In defining the themes, the researcher clearly articulated the focus of each theme and assessed how each contributed to an overall understanding of the data. This process aimed to maximise the analytical and academic value of the findings. A key component involved developing concise yet descriptive labels for each theme that captured the essence of the issues, including what was occurring, how it occurred, and why it was significant. This helped to distil complex information into coherent categories that facilitate meaningful interpretation and discussion.
6	Write-up	The final stage involved the systematic reporting of the thematic analysis. The chapter begins with an introduction that outlines the research focus, objectives, and methodological approach. The methodology section details the data collection procedures, which in this study involved semi-structured interviews and thematic analysis. Each theme is then presented separately in the findings section, supported by empirical data excerpts as evidence. The analysis considers both the frequency and the significance of the identified themes. Finally, the chapter concludes by summarizing the key findings and demonstrating how the study has addressed the research questions.

Source: Braun & Clarke (2016)

3.5 Reliability, Validity and Saturation

The concept of dependability is widely recognized as a fundamental criterion for assessing reliability in qualitative research. Unlike quantitative research, where reliability often refers to the consistency of measurement instruments, dependability in qualitative research emphasizes the stability and consistency of data over time and conditions. To establish dependability, researchers employ multiple techniques, including systematic observation, collection of real-time and first-hand information regarding recurring events, and comprehensive documentation of processes and findings. Triangulation is another essential strategy, involving the use of multiple data sources, methods, or investigators to cross-verify information, thereby enhancing the robustness of the results.

Additionally, the integration of interview sessions allows for deeper insight and reflexivity, where the researcher continuously reflects on their role, biases, and the research process itself to mitigate subjective influence and ensure accurate interpretation of informants' experiences. The central aim of these strategies is to guarantee that the findings are consistent, trustworthy, and credible, accurately reflecting the lived experiences and perspectives of informants. Equally important is the practice of transparent decision-making throughout all phases of the research. This transparency not only strengthens the credibility of the study but also supports the possibility of replication or audit by other researchers, which is crucial for validating qualitative findings.

Data saturation is another critical concept within this study, referring to the point during data collection and analysis when no new themes, insights, or information emerge from additional data. Achieving saturation indicates that the data gathered sufficiently captures the complexity and breadth of the research phenomenon, thus fulfilling the research objectives comprehensively. It serves as a methodological safeguard, signalling that further data collection would be redundant and unlikely to contribute additional understanding, thereby optimizing resource use and maintaining research rigor. The determination of saturation is inherently subjective and requires careful judgment by the researcher, informed by continuous data analysis and comparison.

A hallmark of qualitative research is the explicit articulation of the methodologies and techniques used to ensure reliability and validity. Detailed

documentation of these procedures provides transparency, allowing readers to comprehend the researcher's epistemological stance and methodological rigor. This transparency bolsters the credibility and trustworthiness of this research, especially when positioned within the positivist paradigm, where rigor and systematic inquiry are highly valued. Key tenets underpinning credible qualitative research include ongoing critical self-reflection by the researcher regarding potential biases and influences, openness and honesty in reporting processes and findings, ethical responsibility toward informants and data, and an organized, systematic approach to conducting and evaluating research (Yusof & Ahmad, 2021). To uphold these principles, researchers are encouraged to maintain meticulous records throughout the investigation, including field notes, coding logs, decision trails, and memos, which collectively serve as an audit trail (Reynolds et al., 2011).

In contemporary organizational contexts, qualitative research offers a flexible and responsive approach that is well suited to capturing the dynamic and complex nature of workplace phenomena. It enables organizations to gain nuanced insights into evolving cultural structures, social interactions, and organizational behaviours that may not be accessible through quantitative methods alone. By employing a case study design, this research can explore relationships, processes, and phenomena in their natural context, providing rich, detailed understanding. This methodological choice facilitates the integration of qualitative and mixed methods approaches, allowing for triangulation and a more holistic examination of the research questions (Garcia & Gluesing, 2013). Ultimately, qualitative research equips organizations with valuable knowledge that can inform practice, policy development, and strategic decision-making in real-world settings.

3.6 Research Ethics Approval

Ethical integrity is a fundamental requirement in qualitative research, particularly when human participants are directly involved in data generation. As this study required interviews with organizational employees and involved access to internal information related to AIS and ICG, formal ethical approval was obtained prior to any field engagement.

Approval to conduct this research was granted by the Research Ethics Committee (REC) of Universiti Teknologi MARA on 10th April 2023 as shown in

Appendix B below, ensuring that the study adhered to ethical standards relating to informant welfare, informed consent, confidentiality, and responsible data handling. This process involved the submission of detailed documentation outlining the research objectives, recruitment approach, interview protocols, data protection measures, and strategies for safeguarding informant anonymity and organizational confidentiality.

All informants were briefed on the purpose and scope of the study and were required to provide informed consent prior to participation. Participation was strictly voluntary, and individuals retained the right to withdraw at any stage without consequence. No personal identifiers, sensitive financial information, or proprietary data are disclosed in this thesis, in compliance with research ethics policy and the Personal Data Protection Act 2010 (PDPA). To further ensure ethical compliance, organizations involved in this study are anonymized as Company A and Company B. All interview recordings, transcriptions, and documents were stored securely and accessed only for research purposes. These measures affirm the ethical responsibility undertaken throughout the research process and uphold research transparency, participant protection, and academic accountability.

3.7 Chapter Summary

This chapter is structured to present the overall research design that underpins this study. It provides a comprehensive explanation of the methodological framework, including the philosophical assumptions that guide the research paradigm, the qualitative approach adopted, and the specific methods employed in data collection and analysis. The chapter outlines the entire research process, beginning with the formulation of the research questions, followed by the selection of informants, data collection procedures, and concluding with the steps taken during thematic data analysis. Emphasis is placed on maintaining academic rigor, addressing ethical considerations, and ensuring the trustworthiness of the study through transparency and methodological coherence.

In addition to detailing the methodology, this chapter introduces and justifies the use of Trade-Off Theory as the principal theoretical foundation for the study. Trade-Off Theory is regarded as the most appropriate for this context. This is due to its focus on the decision-making tensions and competing priorities that individuals face within organizational systems. Given that users of AIS must constantly navigate conflicting

demands involving control, efficiency, risk, and compliance, Trade-Off Theory offers a robust lens through which the challenges of ICG can be critically examined.

This theoretical framework supports an exploration of the real-world trade-offs experienced by AIS users in multinational corporations. These users are often placed at the intersection of compliance expectations, policy enforcement, and day-to-day operational execution. Trade-Off Theory captures the complexity and nuance of their roles better than more rigid or hierarchical theories. It facilitates an understanding of how users balance expectations from various stakeholders, manage information flow, and respond to both the formal controls embedded in the AIS and the informal demands of their roles.

The selection of two private companies namely Company A and Company B that serves to contextualize these issues within real organizational environments. Both companies are part of larger multinational entities with over 35 subsidiaries across multiple continents, and their AIS and ICG structures reflect this global complexity. This study focuses on subsidiaries operating in Malaysia, the Philippines, Indonesia, Japan, and Singapore, where cultural, regulatory, and organizational diversity can influence the implementation and perception of internal controls.

The next chapter presents the findings from Company A, specifically highlighting the experiences of AIS users and the dilemmas they face in the context of ICG. It explores how these individuals interpret, adapt to, and sometimes challenge internal controls while fulfilling their responsibilities. These insights will contribute to a deeper understanding of the operational realities of ICG and the practical implications of AIS usage in complex organizational structures.

CHAPTER 4

CASE STUDY OF COMPANY A

4.1 Introduction

This chapter outlines the findings in relation to Section 1.4 RO and Section 1.5 RQ. It presents the empirical finding derived from Company A, which represents the first unit of analysis in this study. The chapter begins with an overview of the organisation's structural environment, followed by a description of the AIS user profile and the sources of data obtained for analysis. This foundation provides the contextual background necessary to understand how ICG operates within the company's AIS.

Accordingly, Section 4.3 outlines the organisational and informant context, followed by Section 4.4 which presents the classification of data sources used in this case study. Sections 4.5 describes the ICG practices implemented in Company A's AIS. Section 4.6 then examines which of these ICG practices create dilemmas for AIS users, while Section 4.7 details the dilemmas experienced by users in relation to these practices. Finally, Section 4.8 presents the strategies users adopt to mitigate these dilemmas, highlighting behavioural adaptations, compliance mechanisms, and workflow adjustments.

This chapter concludes with a summarised interpretation of the Company A case before progressing to Chapter 5, which presents Case Study Company B, leading into the cross-case analysis in Chapter 6.

4.2 Background of Company A

Company A is a foreign-incorporated entity registered with the Companies Commission of Malaysia. It is located at the Bayan Lepas Free Industrial Zone in Penang, Malaysia, and is wholly owned by a parent company headquartered in Singapore. The establishment of Company A in Malaysia forms part of the group's regional manufacturing strategy, with operational control and strategic direction exercised by the parent company. As illustrated in Figure 4.1, Company A is one of 35 subsidiaries operating globally under the same Singapore-based holding group. According to the informants, the company's location in the Bayan Lepas industrial area provides strategic access to industrial infrastructure, logistics facilities, and a skilled

technical workforce that supports its manufacturing operations. Company A is principally engaged in the manufacturing of steel pipes for industrial applications.

Each subsidiary, including Company A, is required to submit periodic trading and financial reports to the parent company. Informants explained that this reporting structure enables centralized financial monitoring, performance evaluation, and strategic coordination across the group. As the primary funding source is provided by the holding company, operational decisions at the subsidiary level are closely aligned with cost management and profitability targets determined at group level.

The management of financial and operational data within Company A is subject to multiple layers of security controls, internal policies, and system-based restrictions. Informants described that access to systems, approval authority, and reporting responsibilities are tightly regulated to ensure centralized oversight. Company A also operates under Licensed Manufacturing Warehouse (LMW) status, which allows the company to import raw materials for production under specific customs controls and compliance requirements. At the time of data collection, Company A employed between approximately 500 and 1,000 personnel across production, engineering, finance, logistics, and administrative functions. This workforce size reflects the company's scale of operations and its significance as one of the major manufacturing entities within the Bayan Lepas industrial zone.

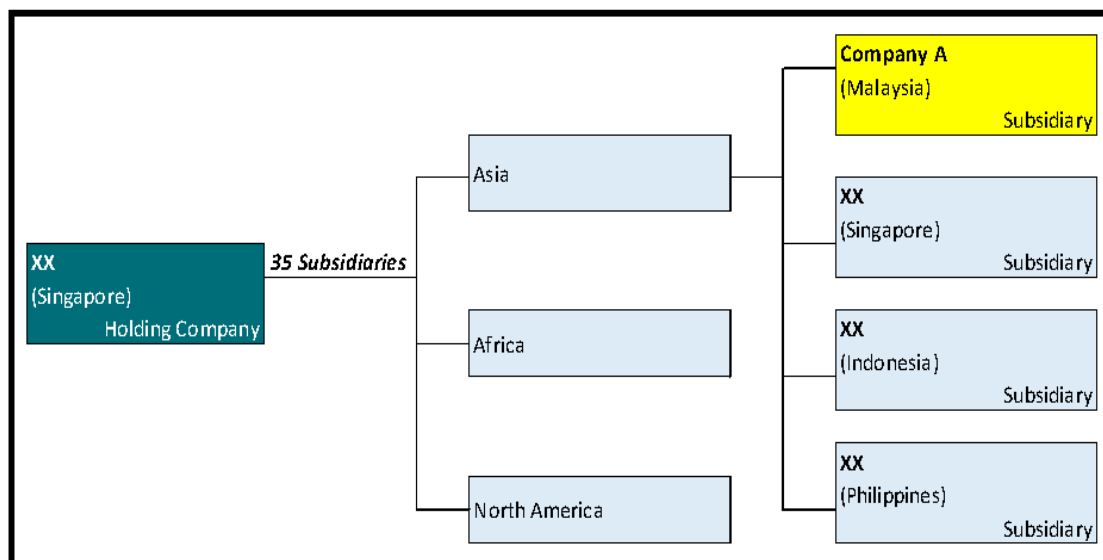


Figure 4.1 Organization Group Structure of Company A
Source: Company A (2026)

4.3 Organizational and Informant Context of Company A

As a distinct legal entity, Company A maintains its own organizational structure, as illustrated in Figure 4.1 above. This structure adopts a top-down hierarchical model that delineates the chain of command and outlines how various activities are coordinated to achieve the organization's strategic objectives under the oversight of its Board of Directors. The demographic profile of the company's workforce is presented in Table 4.1, while Figure 4.2 illustrates the organisational chart, with the informants selected for interviews highlighted in green. These individuals represent users of the AIS and occupy roles that place them under heightened scrutiny due to their access to sensitive financial data.

The individuals marked in green within the organizational chart are directly involved with AIS and are subject to rigorous oversight from both IT governance and CG mechanisms. This intensified monitoring stems from their responsibilities involving the processing and management of interrelated confidential financial information. Their roles require active participation in IT governance procedures and CG frameworks. These positions include the HR manager, HR executive, CFO, finance manager, finance executive, finance assistant, IT manager, and IT executive. Given the varied levels of authority within the organizational hierarchy, it is imperative for the company to implement robust internal control mechanisms within its AIS practices to ensure accountability and safeguard the integrity of business operations.

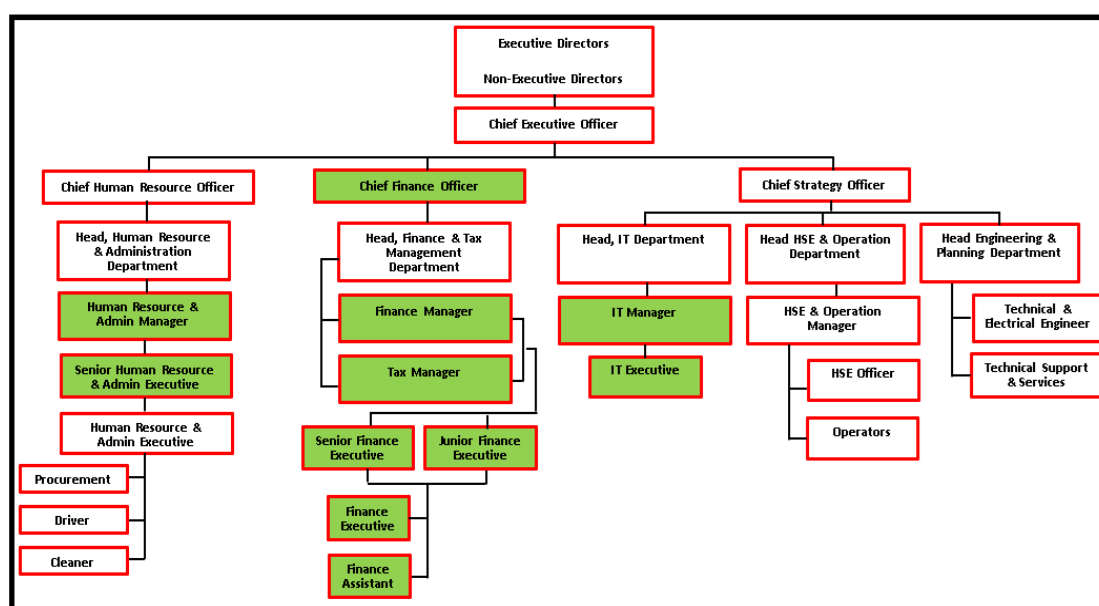


Figure 4.2 Organization Chart of Company A
Source: Company A (2026)

The following subsections outline the structural composition of the organization, the demographic background of AIS users and the distribution of informants who contributed to this case. This context establishes the foundation upon which the subsequent analysis of ICG and AIS dilemmas is developed.

4.3.1 Organizational Structure

Company A employs a top-down hierarchical command system, as illustrated in Figure 4.2, where authority and accountability flow through defined reporting levels. In this structure, personnel associated with finance, IT and human resources perform high-sensitivity transactional work, positioning them within the primary governance oversight scope. The individuals marked in green in the organizational chart represent the study informants, selected because of their operational engagement with AIS-related tasks such as data processing, approval handling, and information security compliance.

The structural placement of these informants determines how they experience internal control demands, SoD and monitoring intensity. Their workflow exposure makes their insights crucial in exploring how ICG influences daily performance, decision latency, and operational judgment within AIS-dependent environments. This structural analysis serves as the foundation for outlining the demographic makeup of AIS users at Company A, which will be discussed in the following subsection.

4.3.2 Demographic Profile of AIS Users in Company A

A total of fourteen informants from Company A participated in this research, comprising senior and mid-level functional positions across finance, tax, IT and HR divisions (refer to Table 4.1). The experienced group with six respondents recording between six and ten years of tenure and eight respondents exceeding ten years of service. The tenure maturity indicates an elevated level of system familiarity, enabling respondents to articulate how governance protocols either facilitate or hinder operational performance.

Such demographic representation enhances the reliability of insights gathered throughout this case study, particularly in analysing control practices, work pressure, and the emergence of user dilemmas under ICG frameworks.

Table 4.1
Informant Demographics of Company A

Designation	No. of Informants
CFO	1
Finance manager	1
Tax manager	1
Senior finance executive	2
Junior finance executive	2
Finance assistant	3
IT manager	1
IT executive	1
HR & Admin manager	1
Senior HR & Admin executive	1
Total Informants	14

Source: Developed for the Current Study

Building upon this experience-based profile, the next subsection further categorises informants through gender distribution to present a transparent participant overview.

4.3.3 Gender Distribution

The demographic analysis also considers the gender composition of Company A informants. Gender representation contributes to a more complete understanding of organisational participation, especially when evaluating workplace practices, access privileges, and perception toward ICG. Out of fourteen AIS-related informants in Company A, six (6) were male and eight (8) were female, as summarised in Table 4.2.

This distribution indicates that female users constitute a slightly larger representation in AIS-linked functions, particularly within finance-related roles, whereas male users are primarily concentrated in IT-related positions. Diversity in demographics strengthens the reliability of the findings by presenting balanced user experiences across governance interactions.

Table 4.2
Gender of the Interview

Gender	Frequency	Percentage (%)
Male	6	43%
Female	8	57%
Total	14	100%

Source: Developed for the Current Study

Having established the organisational and demographic context of Company A, the next section systematically presents the summary of data sources, including document reviews and interview informant codes. This structural clarity ensures transparency in evidence tracing and reinforces validity for subsequent thematic discussions in Sections 4.5 to 4.7 below.

4.4 Summary of Data Sources for Company A

This section summarises the qualitative evidence obtained from Company A through document review and semi-structured interviews. To enhance credibility and provide an accurate picture of organisational reality, data triangulation was used, avoiding reliance on interpretations from only one source. Documents were coded using the prefix DCA (Document–Company A), while interview informants were assigned codes beginning with ICA (Informant–Company A). Coding was used to keep information confidential, make it easier to track evidence, and ensure consistent citation in the findings chapter.

The dataset consists of five internal organisational documents and fourteen interview informants across multiple functional areas involved in AIS operations and ICG. Each data source is categorised by its type, issuing authority, year of access, job role, and scope. This organisation helps clarify which evidence backs each theme during later analysis.

4.4.1 Interview Informant Codes

Codes for interviewing informants were designated according to their level of responsibility in the hierarchy and how closely their roles related to AIS. By substituting personal details with codes, references to evidence can be made neutrally during the discussion of findings. The first two characters denote Company A

informants (ICA), followed by a numerical sequence that represents the order of interviews.

Table 4.3
Interview Informant Codes of Company A

Informant Code	Position / Job Level	Department	Years of Experience
ICA01	CFO (Senior Management)	Finance	> 10 years
ICA02	Finance Manager	Finance	> 10 years
ICA03	Tax Manager	Finance	> 10 years
ICA04	Senior Finance Executive	Finance	6–10 years
ICA05	Senior Finance Executive	Finance	6–10 years
ICA06	Junior Finance Executive	Finance	6–10 years
ICA07	Junior Finance Executive	Finance	6–10 years
ICA08	Finance Assistant	Finance	6–10 years
ICA09	Finance Assistant	Finance	6–10 years
ICA10	Finance Assistant	Finance	6–10 years
ICA11	IT Manager (Senior Level)	IT	> 10 years
ICA12	IT Executive	IT	> 10 years
ICA13	HR & Admin Manager	HR	> 10 years
ICA14	Senior HR & Admin Executive	HR	6–10 years

Source: Developed for the Current Study

To contextualise how these users engage with AIS, the next subsection classifies informants by department, function, and job scope

4.4.2 Department, Role and Job Scope Classification

The fourteen informants represent three primary governance-linked operational units: Finance, IT, and HR. Finance contribute the majority portion of AIS users, reflecting the strong association between accounting information processing and transactional control activities. IT acts as technical custodian of system rules, cyber-security, and access monitoring, while HR governs payroll-related entries and user authorisation.

Table 4.4
Department, Role and Job Scope Classification

Department	Role Category	Job Scope Summary
Finance	Operational Execution Roles	Financial reporting, transaction processing, audit trail handling
IT	System Control & Access Governance	System configuration, authentication, cyber risk monitoring
Human Resource	Compliance & Administration Governance	Employee records, access rights coordination, PDPA compliance

Source: Developed for the Current Study

The distribution of job scopes shows dual governance responsibility: Finance controls operational accuracy, while IT ensures systemic integrity and security. HR's involvement completes the control cycle through authorisation and employee record updates. Beyond human participation, documentary sources further triangulate internal control processes. The following section outlines the organisational documents coded for analysis.

4.4.3 Document Source Codes

The documentary evidence for Company A was examined using a structured coding approach to facilitate traceable interpretation. Each document was assigned the prefix DCA to denote Document Company A, followed by a sequential number representing the order of extraction and review. The documentation spans operational, financial and governance domains, reflecting both strategic direction and procedural execution within the AIS environment. These official records enhanced the richness of interview findings by enabling verification of policies through written rules, reporting structures, and procedural guides.

Table 4.5
Document Source Codes of Company A

Document Code	Title of Document	Issuing Department	Last Updated	Relevance to the Study
DCA01	Business Model	Strategic Management Division	2025	Provides organizational purpose, core activities, and AIS reliance for strategic execution.
DCA02	Corporate Structure	Corporate Secretariat	2022	Clarifies governance hierarchy, reporting flow, and ICG authority delegation.

DCA03	Organizational Charts	Human Resource Department	2024	Maps job roles and reporting lines of AIS users relevant to ICG interaction.
DCA04	Financial Reports	Finance Department	2025	Confirms financial control checkpoints and evidence audit trail embedded in AIS.
DCA05	Policies, Rules, and Guidelines	Internal Governance Compliance and IT Unit	2024	Identifies ICG frameworks including approvals, duty segregation, system authorization and etc.

Source: Developed for the Current Study

With the data sources clearly established and categorised, the next section proceeds to present the findings for Company A based on thematic coding of both documentary and interview evidence. Section 4.5 begins by analysing how ICG operates within the AIS environment of Company A, followed by identification of factors that shape user experiences, organisational behaviours, and dilemma formation in daily system interaction.

4.5 ICG Practices in AIS of Company A

ICG within the AIS of Company A is fundamental to ensuring accurate financial reporting, operational efficiency, and compliance with regulatory requirements. Contemporary frameworks, such as the updated COSO model, emphasize the importance of risk management and accountability in internal controls to safeguard organizational objectives (COSO, 2020). In the Malaysian context, internal control practices must align with the regulations and industry-specific standards, particularly for LMW entities like Company A (SSM, 2020).

Company A implements fundamental control across all organizational levels, from the Board of Directors to operational employees. ICG practices such as **Information Classification and Handling**, **Acceptable Use of IT/AIS**, and **Alignment with Core Organizational Value** define how financial and operational information should be managed, shared, and protected. These policies ensure that employees handle sensitive data appropriately while adhering to organizational ethical standards and transparency principles. Such governance mechanisms promote a culture of accountability and reinforce the organization's commitment to responsible information management.

In terms of access governance, Company A applies structured mechanisms to regulate how users interact with the AIS. Controls including **User Access Management**, **Role-Based Access Control**, **Password and Authentication Standards** and the **Access Authentication Requirement** ensure that only authorized personnel can access financial systems and perform designated tasks. These mechanisms follow the principle of least privilege, whereby system permissions are granted according to job roles and verified through secure authentication procedures. By controlling the lifecycle of user access from onboarding to termination, the organization minimizes the risk of unauthorized access or misuse of financial information.

To further safeguard financial transactions, Company A emphasizes fraud prevention through operational control mechanisms. **SoD** remains a cornerstone of ICG at Company A, ensuring no individual holds excessive control over transactions. For example, initiation of financial transactions by lower-level staff requires approval by supervisors and authorization by senior management, including the CFO. Likewise, IT changes must pass through multiple authorizers, reinforcing checks and balances. In addition, **Privileged Access Control** restricts administrative system privileges to authorized personnel, while **Audit Trail and Log Retention** and **Automated Audit Trail Enforcement** ensure that all transactions and system activities are automatically recorded and preserved for accountability and audit purposes. These controls collectively enhance traceability and support internal and external audit processes.

From a cybersecurity and infrastructure perspective, Company A adopts several technological safeguards to protect the AIS environment. Controls such as **Remote Access Controls**, **Endpoint Security Controls**, and **Monitoring and Surveillance Controls** enable the IT department to regulate remote connectivity, secure endpoint devices, and continuously monitor system activities for suspicious behaviour. These security measures are essential in mitigating cybersecurity risks and preventing unauthorized access to confidential financial information, particularly as organizations increasingly rely on digital platforms and remote operations.

In addition to internal system safeguards, Company A governs the management of data and external interactions through structured data governance practices. Controls such as **Data Retention and Disposal**, **Email and External Sharing Controls**, and **Third-Party or Vendor Access Controls** regulate how financial information is stored, shared, and accessed by external stakeholders. These practices ensure that sensitive

information is retained according to regulatory requirements while preventing unauthorized disclosure or misuse by external parties.

To reinforce compliance and governance awareness, Company A also emphasizes organizational learning and enforcement mechanisms. **Compliance Training and User Awareness** programs are continuous employee training, clear role documentation, and internal audits to improve adherence to control procedures and reduce compliance risks. At the same time, **Disciplinary and Enforcement Mechanisms** establish clear consequences for violations such as unauthorized system access or policy non-compliance. These measures help strengthen governance culture and ensure that employees remain accountable for their actions within the AIS environment.

Despite the comprehensive implementation of ICG practices, AIS users frequently encounter operational challenges when navigating these controls. Employees, particularly those in finance and IT roles, must balance strict compliance with governance procedures while simultaneously meeting operational deadlines and performance targets. This tension may create dilemmas in decision-making, where users must choose between procedural compliance and operational efficiency. Such challenges highlight the importance of designing governance frameworks that remain effective without imposing excessive operational constraints.

Table 4.6
Department, Role and Job Scope Classification

ICG Practices			Description
Acceptable Use of IT/AIS			Defines permitted and prohibited activities when using AIS and organizational systems.
Access Requirement	Authentication		Requires identity verification before users can access AIS resources.
Alignment with Organizational Value	Core		Ensuring AIS practices reflect organizational ethics, integrity, and transparency principles.
Audit Trail & Log Retention			Maintains system logs of user activities and transactions for audit and compliance purposes.
Automated Enforcement	Audit Trail		Automatically records system activities and transactions for accountability.
Backup, Recovery & Continuity	Business		Ensures data backup, disaster recovery, and system continuity during disruptions.
Change Management Configuration/Updates)	(System		Requires approval and testing before system changes are implemented.

Compliance Awareness	Training & User	Provides training to strengthen employee awareness of security and compliance responsibilities.
Data Retention & Disposal		Defines retention periods and secure disposal procedures for AIS data and records.
Disciplinary Mechanisms	/ Enforcement	Defines corrective actions and penalties for violations of AIS policies and controls.
Email / External Sharing Controls		Restricts external sharing of sensitive financial information.
Endpoint Security Controls		Protects endpoints through antivirus, device hardening, and regular patch updates.
Incident Reporting & Response		Establishes procedures for reporting and managing security or system incidents.
Information Handling	Classification &	Classifies data and establishes rules for secure storage, transmission, and sharing.
Monitoring & Surveillance Controls		Continuously monitors system activities to detect suspicious behaviour.
Password & Authentication Standards		Enforces strong password policies and multi-factor authentication for secure system access.
Privileged Access (Admin/Superuser)	Control	Restricts and monitors of high-level administrative system access.
Remote Access Controls (VPN / Secure Access)		Regulates secure remote access through VPN and network security protocols.
Role-Based Access Control		Assigns system permissions based on job roles to enforce the “need-to-know” principle.
Segregation of Duties		Separates critical transaction responsibilities to reduce risks of fraud or error.
Third-Party / Vendor Access Controls		Controls and monitors vendor access to AIS systems and data.
User Access Management		Controls user access requests, approvals, modifications, and revocation throughout the employee lifecycle.
Vulnerability & IP Protection Control		Protects proprietary systems, software, and intellectual property from unauthorized access or misuse.
Vulnerability Management		Conducts regular vulnerability assessments and remediation to mitigate system risks.

Source: Developed for the Current Study

In summary, Company A has implemented a broad range of ICG practices within its AIS to safeguard data integrity, strengthen accountability, and ensure compliance with organisational and regulatory requirements. These practices reflect alignment with recognised governance and control principles and demonstrate the organisation’s commitment to maintaining robust financial and information controls. However, the presence of multiple and layered controls also means that not all ICG practices affect AIS users in the same way during daily operations.

Importantly, empirical evidence from interviews indicates that only a subset of these ICG practices gives rise to recurring operational and behavioural dilemmas for AIS users. While many controls function effectively as preventive or detective mechanisms, certain practices exert greater pressure on users due to their direct impact on access, workflow dependency, traceability, and performance expectations. Accordingly, the next section narrows the analysis to four specific ICG practices that were consistently identified by informants as sources of dilemma by examining how these practices shape user experience, decision-making, and operational tension within the AIS environment.

4.6 ICG Practices Creating AIS User Dilemmas of Company A

This section presents four dominant ICG practices identified in Company A and explains how they generate dilemmas for AIS users in real working conditions. Evidence was derived from fourteen informants across Finance, IT, and HR functions. To demonstrate analytical validity, each theme is supported by multiple quotations, marked with informant codes and number of contributors. The findings answer RO1 and RQ1, which seek to determine what types of ICG practices create dilemmas and how they emerge within daily AIS usage. These mechanisms include: (a) vulnerability and IP Protection Controls, (b) access authentication requirement, (c) automated audit trail enforcement, (d) alignment to core organisational value.

4.6.1 Vulnerability and IP Protection Controls

In Company A, access to sensitive production information such as steel grade composition, pipe thickness specifications, welding procedures, machine calibration settings, and tender pricing documents is restricted exclusively to senior-level personnel through SoD. These controls are intended to prevent data leakage, protect intellectual property, and maintain competitive advantage in the steel pipe manufacturing market. However, the same protection also creates a dilemma when workflow depends on individuals with high-level access.

Several AIS users reported that daily operations often pause during peak periods because approvals or system clearance cannot proceed without authorised personnel. Tasks such as month-end closing, supplier payment processing, material issuance for production and payroll data retrieval may stall while staff wait for signatories. This

results in tension between confidentiality requirements and timely operational output. A shared perspective among informants, who observed:

“A reliable AIS is not just for reporting. It works like a vault. Secure, controlled, and accessible only to certain people. But when approval is urgent and that person is not reachable, work stands still. The system protects, but it delays.” (ICA12)

“Even for simple requests like invoice release or stock transfer, if the authorised user is off-site, everything queues. We understand why access is restricted, but the waiting slows down operations.” (ICA02, ICA07 & ICA09 - collaborative view)

“Month-end closing becomes a race. Figures, journal entries, payment runs. All require clearance, and when only one or two people can approve, it bottlenecks productivity. Security is strong, but the flow is slow.” (ICA04, ICA08 & ICA10 - collaborative view)

Similar concerns were mirrored by other respondents, who reported waiting for clearance to release supplier payments, retrieve design documents, or execute time-sensitive entries. Their accounts collectively suggest that while the control system successfully mitigates unauthorised exposure of proprietary designs, it also introduces workflow stall points that users navigate regularly.

The CFO further explained that risks arise not only from unauthorized access but also from technical vulnerabilities in infrastructure:

“Technical weaknesses come from systems not being maintained or updated. A missed patch or outdated server creates a crack and that crack can lead to data loss or unauthorized access. A small vulnerability in AIS does not stay small. It affects reporting, payroll privacy, even fraud detection.” (ICA01)

The mechanism therefore protects IP and confidential financial assets but creates tension between security strength and workflow continuity. Users recognise the value of tight control yet simultaneously experience slowdown when clearance dependency constrains task execution.

4.6.2 Access Authentication Requirements

AIS access in Company A operates through controlled authentication layers including VPN gateway entry, personalised login credentials, and role-based visibility of modules. These mechanisms strengthen traceability, yet users described the process as time-consuming when multiple verifications are required across remote sites or when

working during production rush periods. In instances where finance staff attempted to retrieve reports from overseas subsidiaries, log-in attempts were repeatedly rejected until regional network clearance was granted. This led to task postponement and reduced collaborative autonomy. A shared perspective among informants, who observed:

“We understand authentication is necessary to prevent unauthorised changes, but when the system keeps asking us to re-login during financial closing, it slows us down. At times, more time is spent on accessing the system than analysing figures.” (ICA02, ICA04, ICA06 & ICA09 -collaborative view)

“Switching modules requires continues re-verification. It protects us from data breaches, yes, but it interrupts concentration and extends processing time. When deadlines are close, it becomes stressful rather than helpful.” (ICA05, ICA07, ICA08 & ICA10 - collaborative view)

This statement underscores the importance of adhering to established authentication protocols to uphold organizational security standards. The IT manager also highlighted the practical importance of user-specific authentication as a security safeguard against unauthorized access:

“It is important that every employee uses their own unique ID when accessing the AIS not just because it is policy, but because it helps us trace activity back to the right person. Think of it like a digital fingerprint. If someone logs in using someone else’s credentials, that is where the problem starts. Without those unique IDs, it would be impossible to know who is doing what in the system, and that opens the door for mistakes or worse, deliberate fraud to go unnoticed. When everyone uses their assigned ID, it allows us to monitor the system more effectively. We can flag suspicious access patterns, review who approved what, and act quickly if something seems off. It is not just about keeping people honest it is about giving management the visibility they need to know when something or someone does not belong” (ICA12)

This highlights the critical role of unique identifiers in monitoring and controlling access to sensitive information, thereby enhancing the organization's ability to detect and respond to potential security threats promptly. In conclusion, the mechanism therefore strengthens governance, yet introduces performance dilemmas such as login dependency, slower task switching, and user anxiety toward traceability especially among junior finance staff who process high-volume transactions daily.

4.6.3 Automated Audit Trail Enforcement

Company A's AIS automatically captures each posting, reversal, adjustment entry, and approval flow. Internal audit and finance rely heavily on this trail to verify accuracy during compliance reviews. Users acknowledged that the system strengthens transparency and minimises undocumented changes. However, the same surveillance encourages caution among employees who worry that errors could be traced directly back to them. This was particularly noted among junior staff handling first-level postings, who described feeling hesitant when system alerts signal potential anomalies.

"The automated audit trail is crucial for us because it documents every user action within the AIS, covering data entry, amendments, and approval steps. This complete traceability allows us to see exactly who did what and when, which increases our confidence in the accuracy and credibility of the financial information. It also helps prevent misconduct, as users are aware that the system records their activities." (ICA06, ICA07 & ICA13 - collaborative view)

"The automated audit trail in our AIS is essential because it captures every action taken by users, not only the transactions themselves. From data entry to corrections and approvals, everything is recorded, giving us a clear and traceable path of who performed what, when, and for what reason. This level of transparency strengthens our confidence in the integrity of the financial records and discourages misconduct, since everyone understands their actions are monitored." (ICA04 & ICA05 - collaborative view)

Likewise, the tax manager emphasized the diagnostic role of the system's backend:

"What people do not always realize is that the real power of the AIS lies in its back end, specifically in the automated audit trail. It is not just about processing transactions quickly or generating reports. The system is constantly monitoring every input and activity behind the scenes. So, when something goes wrong maybe an invoice is posted twice, or a number does not match up, the audit trail allows us to dig deep and trace it back to the source. It tells us who entered the data, when they did it, and even what changes were made over time. This is especially helpful when trying to resolve inconsistencies in data entry. Sometimes errors are unintentional, sometimes they are due to misunderstanding the system, but with the audit trail in place, nothing is invisible. It gives us visibility, accountability, and most importantly, the ability to

correct issues before they become real problems. It is like having a digital safety net that not only catches mistakes but teaches us where our processes or training might need improvement” (ICA03)

These insights underscore how Company A views the automated audit trail not just as a technical feature, but as a governance tool central to safeguarding financial integrity. Yet, they also highlight a key dilemma while automation improves control efficiency, it simultaneously demands a higher level of user competence and confidence. This is something that not all employees possess at equal levels. The case of Company A exemplifies a common ICG challenge in AIS, which involves achieving an optimal balance between reliance on automated controls and the development of user awareness and accountability. It also underscores that the effectiveness of internal control mechanisms ultimately depends on the competence and engagement of users, which is a critical insight in the ongoing discourse on AIS governance.

4.6.4 Alignment With Core Organizational Values

ICG in Company A is communicated not only as a requirement of governance but as a reflection of organisational values. Accuracy, integrity, and transparency are emphasised as non-negotiable work principles. AIS controls function as the behavioural reinforcement of these values through structured approval routing, mandatory documentation, and strict error reporting. Staff noted that the expectation for near-perfect compliance intensifies personal pressure, especially during peak workload where rapid judgment is needed. This sentiment is echoed by CFO, who emphasized the value of reliability in financial records:

“ICG is not only a system. It is a culture. If the data cannot be trusted, all the reporting loses meaning. The value of AIS is in integrity, and we hold our people to that standard.” (ICA01)

The CFO’s comment highlights the intrinsic link between trustworthy data and organizational value creation. For AIS to serve as an effective tool of internal control, it must inspire confidence that the data it processes and reports are complete, consistent, and accurate. This view supports the thesis that users’ understanding and engagement with AIS controls are central to their effectiveness. A shared perspective among informants, who observed:

“The AIS is not just a system for posting transactions. It gives meaning to what the business does. Past records, present decisions, and future projections all become measurable because the system converts activities into numbers. That is why the AIS drives decision-making at top level. It shapes how we interpret results and how we prepare for what comes next.” (ICA02, ICA03 & ICA11 - collaborative view)

“Numbers only matter when they reflect reality. Without proper controls or when users do not follow process, the data becomes unreliable. Once that happens, we lose clarity, responsibility, and alignment with values. AIS is more than accounting software, it shows how seriously we uphold integrity, accuracy, and accountability across the organisation.” (ICA02, ICA13 & ICA41 - collaborative view)

This statement reflects a broader understanding of AIS as a strategic tool as its not merely for record keeping, but as a mechanism for valuing business operations across timeframes. The quote also reinforces the idea that internal controls within AIS must be forward looking, adapting to evolving business contexts while preserving historical integrity and present accuracy. In the case of Company A, while this approach strengthens ethical compliance, employees reported internal tension when value-driven expectations conflict with workload realities or system constraints.

Table 4.7 summarizes the ICG mechanisms in place at Company A, which are obligatory for all AIS users. The thematic derivation of these mechanisms is based on qualitative data collected through interviews and transcripts with Company A’s informants. These findings emphasize that AIS is not only a technical tool but also a vehicle through which organizational values are embedded into everyday financial processes. Thereby, minimizing users' dilemma through alignment, accountability, and clarity.

Table 4.7
Summary on the ICG Practices and Resulting Dilemmas of Company A

ICG Practices		Dilemma Experienced	Supporting Evidence (Informant Codes)
Vulnerability & Protection Control	IP	Restricted access delays workflow and raises dependency on authorized holders	ICA01, ICA02, ICA04, ICA07, ICA08, ICA09, ICA10, ICA12
Access Requirement	Authentication	Multi-layer login slows task execution, especially across subsidiaries	ICA02, ICA04, ICA05, ICA06, ICA07, ICA08, ICA09, ICA10, ICA12

Automated Enforcement	Audit Trail	Alerts increase awareness but create fear of error traceability	ICA03, ICA04, ICA05, ICA06, ICA07, ICA13
Alignment with Organizational Value	Core Value-based compliance pressure for perfect accuracy	increases	ICA01, ICA02, ICA03, ICA11, ICA13, ICA14

Source: Developed for the Current Study

These findings confirm that the identified ICG controls do not hinder AIS use by design, but friction emerges when governance strength intersects with high-speed operational demands. In short, RO1 is fulfilled through the identification of four dominant control practices and the specific dilemmas each produces for users in Company A. While Section 4.6 establishes what practices create tension, Section 4.7 explores the underlying contributing factors that shape these dilemmas, revealing the organisational, technical, and behavioural conditions that influence how AIS users respond to control enforcement.

4.7 Dilemmas Experienced by AIS Users in Relation to ICG Practices of Company A

This study identified three major factors that contribute to dilemmas experienced by AIS users under ICG practices within Company A. These factors emerged consistently across the 14 interview informants and demonstrate how governance mechanisms, while intended to strengthen accountability, simultaneously create operational constraints. The following subsections present these findings in relation to RO2 and RQ2, which seek to examine why ICG-related dilemmas arise, particularly in relation to technological complexity, regulatory expectations, and ethical responsibilities. Five dominant influences emerged consistently across the fourteen informants that include (a) regulatory compliance pressure, (b) cybersecurity control restriction, (c) high security system pressure, (d) bureaucratic procedures from SoD, and (e) technology-related performance anxiety. These influences shaped how users interpreted internal controls, responded to procedural restrictions, and navigated internal conflicts when making decisions in their daily tasks. The subsections below present each dilemma experienced by AIS users supported by explanation and interview extracts.

4.7.1 Regulatory Compliance Pressure

Company A operates in a structured regulatory environment where compliance requirements guide financial processing, documentation, audit readiness, and reporting accuracy. The interviews showed that while AIS serves as a tool to enforce compliance, it also restricts individual discretion, creating dilemmas between speed and procedural correctness. Users described feeling torn between meeting submission deadlines and ensuring detailed supporting documentation for every transaction. This means they often operate under the pressure of accountability obligations that cannot be compromised for convenience or speed.

Several informants collaborated in explaining that external audit cycles intensify this compliance pressure, especially when auditors demand justification for entries, recalculations, or transaction trails. Users reported that closing accounts becomes stressful when verification procedures extend beyond planned deadlines, forcing them to balance organisational expectations with audit integrity.

“Sometimes we are scared to post even a small transaction because everything must be justified. One mistake means we need to refile, so we move slower to avoid trouble.” (ICA01, ICA03 & ICA06 - collaborative view)

“The compliance checklist is long, and every entry need evidence. I understand the purpose, but it adds a layer that slows daily tasks especially when deadlines are tight.” (ICA07 & ICA11 - collaborative view)

“We try to close accounts fast, but the regulatory steps hold us. We cannot skip or shorten anything even if it is urgent.” (ICA10 & ICA12 - collaborative view)

Overall, regulatory requirements protect reporting integrity but simultaneously reduce operational flexibility, leaving users to negotiate between meeting deadlines and maintaining audit-proof records. This dilemma contributes directly to tension under ICG and leads into the second factor, where control extends into digital security.

4.7.2 Cybersecurity Control Restriction

Cybersecurity monitoring in Company A is conducted quarterly and is integrated directly with AIS functions. Staff described how routine claims, reimbursements and data management occur through the system, allowing HR to verify receipts, mileage and supporting documents. While this prevents misuse, it also

introduces scrutiny and extended approval time, particularly when claims exceed limits or require evidence resubmission.

Centralised filing was seen as efficient and fair, but also restrictive when files needed amendments or when network alerts slowed processing. Interviewees collaborated that system-integrated monitoring improves traceability but reduces autonomy in simple transactions.

“We cannot see certain reports unless approved by higher access. If the person is on leave or busy, we must wait. It is secure but slows our flow.” (ICA02, ICA05 & ICA10 - collaborative view)

“The cybersecurity control is tight. I know it protects the company but sometimes we just need quick reference, and the restriction becomes a barrier.” (ICA04 & ICA08 - collaborative view)

“Every request for access needs justification. This protects data but delays troubleshooting, especially when we need to solve something on the spot.” (ICA12 & ICA14 - collaborative view)

In practice, cybersecurity monitoring improves accountability but introduces a procedural burden that users must balance with task urgency. This leads into the next dilemma source, where risk controls extend to fraud prevention.

4.7.3 High Security System Pressure

Recurring payments to suppliers heightened concerns about possible manipulation, leading the company to require layered approval and document verification within AIS. Interviewees explained that approval cannot proceed without a purchase order, delivery record, and invoice match, which mitigates fraud but slows recurring transactions.

Several informants collaborated that system configuration must suit organisational workflow or risk generating confusion and duplicate payments:

“When alerts pop up, we become extra careful. A small wrong entry is visible. This makes us double check everything and our work slows down.” (ICA03 & ICA06 - collaborative view)

“The audit trail is good for transparency but sometimes creates fear because anything we do is recorded. We hesitate before we click submit” (ICA07, ICA08 & ICA13 - collaborative view)

“I feel the system watches us all the time. It prevents fraud but also pressures us to be perfect which is unrealistic during peak task periods” (ICA04 & ICA09 - collaborative view)

Fraud and risk oversight therefore reduces financial exposure but adds procedural layers that users must navigate daily. The following subsection presents how SoD further influences this dilemma.

4.7.4 Bureaucratic Procedures From Segregation of Duties

SoD was described as one of the tightest control points within AIS. Interviewees noted that the person initiating a transaction cannot verify or approve it, and approvals must occur before execution. This prevents unauthorised transfers but results in processing delays when multiple approvers are unavailable.

“We need different people to approve and sometimes the person is not free. It stops us from completing the task even when everything is ready.” (ICA01 & ICA02 - collaborative view)

“Segregation makes sure no single user controls everything, but we spend time chasing for approval. It delays posting and month-end tasks.” (ICA04, ICA05 & ICA10 - collaborative view)

“If one level of authorisation is missing, the entire process stops. The control is strong, but efficiency is affected.” (ICA07, ICA09 & ICA12 - collaborative view)

Duty segregation therefore secures financial processes but creates bottlenecks that generate user dilemma when speed and compliance conflict. The next factor concerns how errors are reported when controls fail.

4.7.5 Technology-Related Performance Anxiety

Interviewees described error reporting as a governance requirement linked to transparency. Users carry responsibility to disclose errors with explanation notes and follow correction procedures. While this improves accuracy and protects shareholder confidence, staff acknowledged fear of blame, especially when errors involve deadlines or audit review.

“Reporting mistakes is the right thing, but we worry it might affect relationships. We think twice before escalating issues.” (ICA01 & ICA03 - collaborative view)

“The company wants us to speak up but we fear being labelled or causing tension. Sometimes we silently fix things to avoid conflict.” (ICA11 & ICA13 - collaborative view)

“Corrective action procedures are clear but emotionally heavy. We want compliance yet we also want workplace harmony.” (ICA08 & ICA14 -collaborative view)

This created a dilemma between upholding integrity and maintaining workplace relationships, influencing decision-making behaviour. Taken together, these five factors illustrate how ICG, while ensuring compliance and protection, also constrained execution speed, emotional comfort, and operational flexibility. The following section further discusses how AIS users responded to these constraints, the coping approaches they adopted, and how their choices shaped system-related decisions in daily operations.

Table 4.8 below presents a summary of the key factors contributing to the dilemmas faced by AIS users in relation to ICG within Company A. These themes were derived from the empirical findings gathered through interviews with selected informants from Company A, reflecting the challenges encountered by AIS users in the execution of their daily roles and responsibilities.

Table 4.8
Summary of Dilemmas Experience by AIS User in Relation to ICG Practices of Company A

Theme	Dilemma Experienced	Supporting Evidence (Informant Codes)
Regulatory Compliance Pressure	High reporting standards increase documentation workload, create hesitation in decision execution, and slow month-end processing due to fear of non-compliance errors.	ICA01, ICA03, ICA06, ICA07, ICA09, ICA10, ICA11, ICA12
Cybersecurity Monitoring Restrictions	Restricted access to sensitive data delays task completion and increases dependence on approval holders when information is needed urgently.	ICA02, ICA04, ICA05, ICA08, ICA10, ICA12, ICA14
High Security System Pressure	Continuous system monitoring heightens caution and induces fear of traceable mistakes, causing slower decision-making and repetitive self-verification.	ICA03, ICA04, ICA06, ICA07, ICA08, ICA13, ICA09
Bureaucratic Procedures from Segregation of Duties	Multiple approval layers prevent unauthorized control but cause bottlenecks when approvers are unavailable, affecting task flow and deadline compliance.	ICA01, ICA02, ICA04, ICA05, ICA07, ICA09, ICA10, ICA12

Technology- Related Performance Anxiety	Ethical reporting framework encourages transparency yet creates emotional tension between compliance duty and maintaining interpersonal harmony.	ICA01, ICA03, ICA08, ICA11, ICA13, ICA14
--	--	---

Source: Developed for the Current Study

4.8 Mitigating AIS Users' Dilemmas Related to ICG Practices of Company A

Company A's interview data indicates that AIS users actively adopt several behavioural strategies to mitigate the dilemmas created by ICG practices. These strategies reflect how users negotiate uncertainty, workload pressure and compliance obligations when interacting with the AIS environment. The findings reveal that users frequently rely on personal judgement, peer support, and procedural knowledge to navigate control requirements embedded within the system. While ICG aims to prevent fraud and strengthen accountability, employees often described a continuous need to balance control and practicality, particularly when meeting monthly deadlines, handling cross-company reporting, or resolving unexpected variance adjustments.

The five interconnected mitigation strategies that emerged consistently across informants are (a) regulatory awareness, (b) procedural compliance, (c) corporate culture alignment, (d) reporting discipline, and (e) productivity and performance adaptation. Each theme represents how users rationalise compliance while mitigating the pressures created by audit trails, data security controls, and procedural rigidity.

4.8.1 Regulatory Awareness

Regulatory awareness appeared in all interviews as the most immediate response mechanism. Users reported that when uncertainty arises during system entry or approval, the safest action is to refer to policies and audit guidelines to avoid disciplinary consequences. Multiple informants agreed that policy literacy helps reduce incorrect postings and evidence gaps during audit reviews. The informants described this reliance on policy as a shield against accountability risk, stating:

"We always refer to the handbook when we are unsure because every step is recorded in the system. If there is a mistake, audit can immediately trace it. So, policy knowledge protects us from doing something wrong, even when time is tight." (ICA01, ICA04, ICA06 & ICA09 – collaborative view)

Several informants noted that internalisation of rules also prevents over-reliance on verbal instructions, which may be inconsistent across departments. Informants explained how clarity ensures accountability, particularly during external audit season:

“When we follow written policy, we feel safer because it means there is proof that we acted correctly. It is better than depending on what people say, especially when documents go for checking later.” (ICA02, ICA05, ICA07 & ICA12 - collaborative view)

Others highlighted how policy adherence increases confidence, especially for newer staff navigating approval chains, data uploads, and SoD. One HR officer reflected:

“Following the rules step by step keeps everyone aligned. Even if something goes wrong later, we have shown that we acted within company expectations.” (ICA03, ICA08, ICA10, ICA13 & ICA14 - collaborative view)

Across informants, regulatory awareness surfaced as a shared defensive strategy against audit findings, disciplinary consequences, and documentation ambiguity. Users relied on policy familiarity to protect themselves from non-compliance, especially when system decisions were traceable and reviewable. However, awareness alone does not resolve the operational load that comes with meeting internal expectations. This led to the second theme, where AIS users described how obligation and structured processes shape their behaviour in navigating daily dilemmas, as discussed in Section 4.8.2 below.

4.8.2 Procedural Compliance

AIS users repeatedly shared that procedural obligation shapes how they respond to dilemmas that arise from ICG restrictions. KPIs, SOPs and mandatory steps are followed even when workload is high, or approval queues slow the processing of transactions. The group described obligation not only as compliance, but to stay safe from accountability exposure.

“Our KPIs direct how we work. Even if we know faster ways, we still follow the process because results and evaluation depend on it. Deviating means taking risk.” (ICA02, ICA03, ICA05 & ICA11 - collaborative view)

Several staff noted that training and upskilling are tied to KPI outcomes, creating pressure to complete tasks on time while maintaining accuracy. A junior accountant explained:

“Targets push us to improve, but when many submissions come at once, following every step can slow us down. We cannot skip because performance review checks everything.” (ICA04, ICA07, ICA09 & ICA10 - collaborative view)

Informants also described that structured workflow create rhythm and predictability yet leave little room for judgement when system access is delayed or approvals are pending. A procurement clerk reflected:

“Sometimes we wait for approvals before we can continue, but delivery deadlines are fixed. The process protects the company but slows the work.” (ICA01, ICA06, ICA12 & ICA14 - collaborative view)

In summary, obligation, and process form both a performance motivator and a constraint, shaping how users negotiate speed versus compliance. The next theme explores how cultural expectations further reinforce behavioural alignment in section 4.8.3 below.

4.8.3 Corporate Culture Alignment

Corporate culture in Company A operates as an informal control system that influences decision-making beyond written procedures. Many informants described feeling guided not only by rules, but by a collective expectation to reflect the work ethic of the Singapore headquarters. A shared perspective among informants, who observed:

“Even though we are in Malaysia, how we work is shaped by HQ. We follow their standards, their speed, and their discipline. The culture influences our decisions even when policy does not spell it out.” (ICA01, ICA02, ICA03 & ICA08 - collaborative view)

Collaboration across subsidiaries requires shared norms and professional ethics, particularly during consolidated reporting. Several informants explained that unity ensures consistency across the group but also increases pressure when workload peaks or when local practice differs from HQ expectations.

“All subsidiaries move together. We do not think like one company, we think like one group. So sometimes we adjust how we normally work to match the culture” (ICA04, ICA07, ICA10 & ICA14 - collaborative view)

Management staff added that culture helps bridge differences in regulatory context but simultaneously requires multitasking and adaptation to regional standards. An HR executive revealed.

“We manage dual expectations Malaysian law and Singapore reporting. That makes the job more complex because we cannot focus on just one requirement” (ICA05, ICA06, ICA09, ICA11 & ICA13 - collaborative view)

Corporate culture therefore strengthens accountability yet introduces additional cognitive and procedural demands. The next section examines how these expectations translate into reporting constraints and outcome pressure, as presented in Section 4.8.4.

4.8.4 Reporting Discipline

Reporting standards determine how data accuracy is judged, and informants frequently link reporting quality with audit comfort, management trust, and system credibility. Informants expressed that monthly reporting cycles require high precision, where errors carry reputational risk and workload consequences.

“Reporting quality directly influences management decisions. When the data is accurate, they can plan with confidence, but if the input is wrong, the entire process becomes unreliable. That is why the pressure to ensure correct reporting is so high.” (ICA01 & ICA03 - collaborative view)

“Management relies heavily on reporting quality. If the information entered is accurate, they can make decisions confidently, but any incorrect input causes the whole decision process to fall apart. This creates significant pressure to get the data right.” (ICA04, ICA06 & ICA09 - collaborative view)

Many users mentioned that structured reporting helps trace discrepancies yet increases time consumption when adjustments require multiple approval levels. Informants’ respondent illustrated this dilemma:

“Reports are reliable, but updating a mistake takes long because everything is checked. We feel safe but also slower.” (ICA05, ICA08, ICA10 & ICA12 - collaborative view).

Cross-department informants added that clear formatting and evidence documentation reduces confusion during audit trails and intercompany reconciliation. However, rigid reporting templates leave limited room for judgement when exceptional cases arise:

“Sometimes the situation does not fit the template, but we must still force it in. The structure helps but can restrict us.” (ICA02, ICA07, ICA11, ICA13 & ICA14 - collaborative view)

Overall, reporting standards provide reliability yet intensify pressure for perfection, setting the foundation for the fifth theme where performance outcomes and workload are directly affected. This is further elaborated in Section 4.8.5.

4.8.5 Productivity and Performance Adaptation

The final theme shows that productivity is most affected when users must balance control compliance with workload urgency. Informants consistently voiced that strict internal controls ensure safety but slow down execution when manpower is limited or when approvals bottleneck. Informants highlighted the trade-off:

“Controls protect the company, but they take time. When someone is on leave, we cover extra work to meet deadlines. The system does not slow down, so we adjust.” (ICA01, ICA03, ICA06, ICA10 & ICA12 - collaborative view)

Users explained that performance improves when data input is accurate, reducing reprocessing and correction workload. However, variance review, audit queries and cross-entity reporting contribute to stress during peak cycles. Informants described this operational strain:

“Stress comes when mistakes are found because fixing takes longer than doing right the first time. So, quality input saves work later.” (ICA02, ICA05, ICA07, ICA09 & ICA13 - collaborative view)

Others emphasised that diverse backgrounds and working styles contribute to misunderstanding and require negotiation before task completion:

“Different people think differently. Sometimes this helps problem solving, sometimes it slows us down. We learn to adjust to each other.” (ICA04, ICA08, ICA11 & ICA14 - collaborative view)

Together, these findings show that productivity reflects not only skill, but how users respond to governance pressure, reporting accuracy demands and manpower capacity. Table 4.9 summarises the five behavioural outcomes influencing AIS users under ICG.

Table 4.9

Summary on Mitigating AIS Users' Dilemmas Related to ICG Practices of Company A

Theme	Dilemma Experienced	Supporting Evidence (Informant Codes)
Regulatory Awareness	Policies, rules, and audit guidelines are used as safety boundaries in decision-making.	ICA02, ICA04, ICA07, ICA11, ICA13, ICA03, ICA12, ICA14
Procedural Compliance	KPI compliance and SOP adherence shape safe behaviour during pressure.	ICA05, ICA06, ICA09, ICA10, ICA07, ICA08, ICA01, ICA1
Corporate Culture Alignment	Adaptation to HQ expectations and collaboration support dilemma navigation.	ICA03, ICA04, ICA09, ICA06, ICA12, ICA08, ICA13, ICA10
Reporting Discipline	Accuracy prioritized over speed, with reinforced verification practice.	ICA13, ICA11, ICA01, ICA14, ICA06, ICA02, ICA12
Productivity and Performance Adaptation	Multitasking and workload negotiation maintain output within governance limits.	ICA02, ICA09, ICA06, ICA03, ICA04, ICA08, ICA07, ICA10, ICA14

Source: Developed for the Current Study

4.9 Chapter Summary

This chapter presented an empirical analysis of ICG within the AIS of Company A, drawing from the interpretations and knowledge of 14 informants across finance, HR, IT, and administrative functions. The findings were structured in accordance with the research objectives, enabling a clearer understanding of how internal controls are designed, enforced, experienced, and mitigated by AIS users. Through a structured thematic analysis that integrated interviews, observation notes, and document review, connotation units were identified, grouped into categories, and subsequently merged into major categories that formed the preliminary elements of the conceptual framework. These major categories reflect how AIS users in Company A experience ICG across technological, procedural, and organisational dimensions in a centralised governance.

In line with the comparative case study design, the findings from Company A establish the analytical foundation for examining Company B. Chapter 5 therefore builds directly on the categories developed in Chapter 4, using them as sensitising concepts to guide the interpretation of data collected from Company B. The thematic analysis for Company B follows the same systematic approach, combining interview evidence with observation and document review to refine, extend, or challenge the patterns identified in Company A. This ensures that the findings from Company B do not stand in isolation but instead deepen and enrich the initial understanding generated earlier.

Accordingly, the transition from Chapter 4 to Chapter 5 reflects the intended methodological progression of the study: Company B serves as a refinement stage, where the initial themes derived from Company A are revisited and further developed within a different organisational context. This approach enhances methodological rigour, strengthens cross case comparison, and contributes to the development of a more robust and empirically grounded conceptual framework.

CHAPTER 5

CASE STUDY OF COMPANY B

5.1 Introduction

This chapter presents the empirical findings in relation to Section 1.4 RO and Section 1.5 RQ for Company B, serving as the refinement layer for the earlier Company A analysis. Unlike Chapter 4, which explored how ICG influences AIS users within Company A, this chapter does not develop a new set of themes. Instead, the Company A findings act as the analytical baseline, while Company B is used to:

- (i) Validate what Company A revealed.
- (ii) Reveal similarities or deviations.
- (iii) Strengthen themes with more empirical grounding.
- (iv) Refine categories in preparation for cross-case synthesis in Chapter 6

The purpose of Chapter 5 is empirical to provide data comparison, not final meaning derivation.

5.2 Background of Company B

Company B is a wholly foreign-owned enterprise registered with the Companies Commission of Malaysia (SSM, 2020), strategically located in the Pelepas Free Zone, Tanjung Pelepas Johor, one of Malaysia's largest international shipping and logistics corridors. Operating as one of 35 global subsidiaries under a Tokyo-based parent corporation, Company B serves as a regional hub for leasing, modernising, and maintaining container handling equipment, cranes, and port machinery components.

All subsidiaries are mandated to use a centralised AIS platform linked to the Tokyo headquarters for real-time financial consolidation. This creates a rigorous financial governance environment driven by strong oversight, high audit visibility, and mandatory compliance reporting, conditions ideal for examining ICG - AIS behaviour.

Workforce strength ranges between 500 - 2,000, reflecting a technologically intensive operating environment with significant audit and transaction volume, intensifying internal control pressure on AIS users.

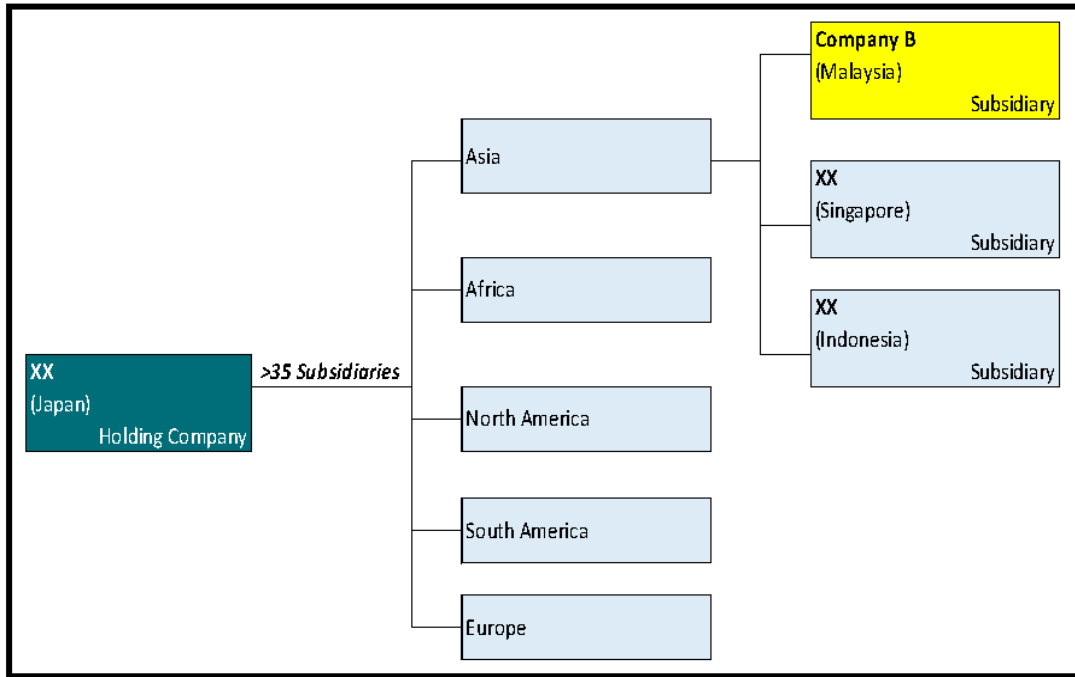


Figure 5.1 Organization Group Structure of Company B
Source: Company B (2026)

5.3 Organizational and Informant Context of Company B

Company B operates under a board-governed structure supported by Finance, IT and HR divisions. The same user clusters observed in Company A. AIS-dependent roles are marked in the organisational chart (Figure 5.1) to indicate internal control exposure points. Users with AIS access include.

Table 5.1
Informant Context of Company B

Department	Positions
Finance	CFO, Finance Manager, Tax Manager, Senior Executives, Junior Executives, Assistants
IT	IT Manager, IT Executive
HR/Admin	HR & Admin Manager, Senior Executive

Source: Developed for the Current Study

These users collectively form a continuous control chain that begins with authorisation, progresses through processing, and extends to system administration and audit trail retention. Each stage of this chain reinforces the next, ensuring that control

responsibilities are distributed, monitored, and traceable throughout the entire AIS environment.

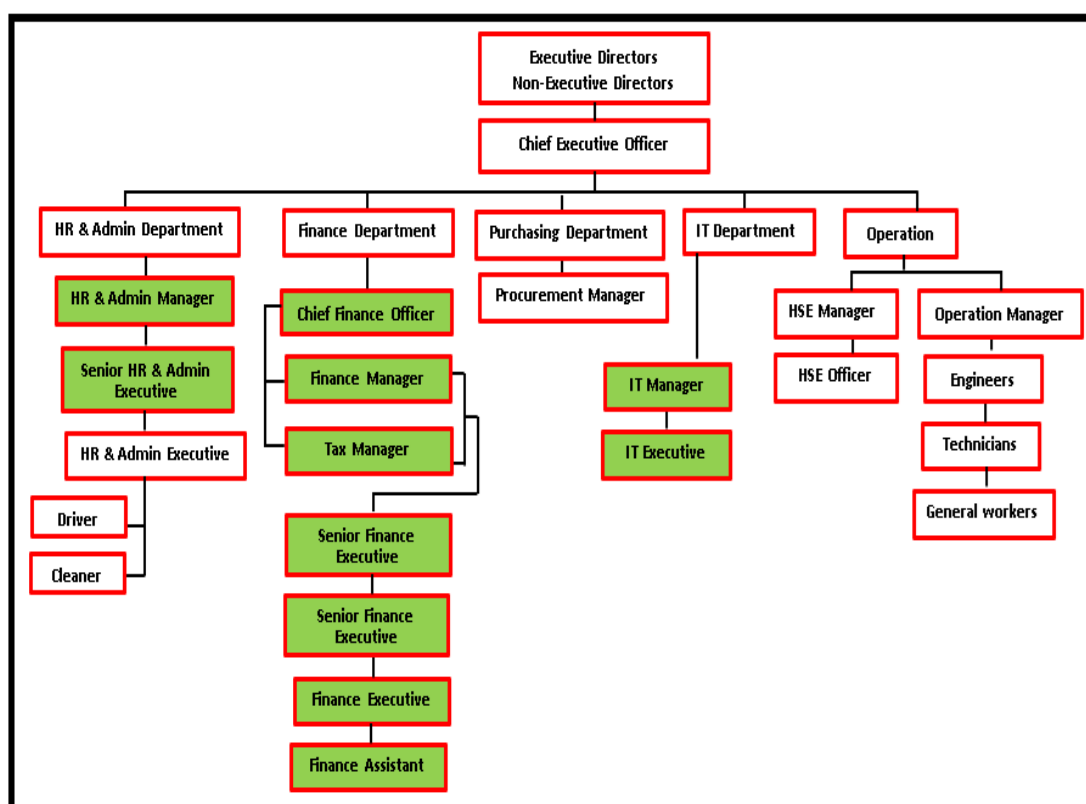


Figure 5.2 Organization Group Structure of Company B
Source: Company B (2026)

5.3.1 Organizational Structure

The structure mirrors Company A with one key difference, control authority is more centralised and Japan-driven, meaning system controls are less negotiable locally.

5.3.2 Demographic Profile of AIS Users

A total of fourteen informants from Company B participated in this study.

Table 5.2
Demographic Profile of AIS Users in Company B

Tenure Group	Count	Implication for Analysis
3–5 years	3	less autonomy, more compliance pressure
6–10 years	5	high system familiarity to evaluate controls realistically

>10 years	6	strong governance memory, can compare policy evolution
-----------	---	--

Source: Developed for the Current Study

Company B has more senior tenure composition, enabling deeper reflection on policy evolution and governance maturity.

Table 5.3
Informant Demographics of Company B

Designation	No. of Informants
CFO	1
Finance manager	1
Tax manager	1
Senior finance executive	2
Junior finance executive	2
Finance assistant	3
IT manager	1
IT executive	1
HR & Admin manager	1
Senior HR & Admin executive	1
Total Informants	14

Source: Developed for the Current Study

Building upon the organisational experience distribution, the next subsection expands the demographic illustration by presenting the gender composition of AIS-related informants.

5.3.3 Gender Distribution

Further demographic analysis was conducted to examine the gender representation of AIS-related users within Company B, as summarised in Table 5.4. This breakdown offers a more holistic view of user participation in internal control environments, where perceptions of authority, system access and control enforcement may vary across demographic lines.

The informant group comprises five (5) male and nine (9) female informants, indicating a higher representation of women within AIS-linked functions, particularly finance and HR. Male respondents were comparatively prominent in IT-centred roles, aligning with common industry staffing patterns observed in technical governance-oriented environments. Such demographic diversity enhances analytical rigour, as findings reflect perspectives drawn from different gender distributions, job scopes, and

exposure levels, providing a more balanced interpretation of internal control pressure, responsibility segregation, and potential governance-related dilemmas.

Table 5.4
Gender of the Interviewees of Company B

Gender	Frequency	Percentage (%)
Male	5	35%
Female	9	64%
Total	14	100%

Source: Developed for the Current Study

With the organisational structure and informant demographics clearly established, the following Section 5.4 summarises the evidence sources employed in this case study, including interview code mapping, document analysis references, and data triangulation procedures used to validate the findings presented in Sections 5.5 to 5.7 below.

5.4 Summary of Data Sources for Company B

This section summarises the qualitative evidence obtained from Company B through document analysis and semi-structured interviews. To strengthen validity, data triangulation was applied across multiple evidence points, ensuring that findings reflect operational reality rather than single-perspective interpretation. All reviewed documents were coded using the prefix DCB (Document - Company B), while interview informants were assigned the code prefix ICB (Informant - Company B).

The coding system was implemented to maintain confidentiality, support systematic traceability, and ensure consistent reference throughout the analysis in Sections 5.5 to 5.7 below.

The consolidated dataset comprises five internal organisational documents and fourteen interview informants, covering operational functions directly related to AIS control, governance enforcement, financial reporting, compliance, and IT administration. Each data source is classified by type, authority, issue year and relevance, illustrating how evidence supports thematic mapping during analytical synthesis.

5.4.1 Interview Informant Codes

Interview informants from Company B were coded according to hierarchical role relevance and involvement in AIS activities. The prefix ICB denotes Informant–Company B, followed by a sequential index representing interview order.

Table 5.5
Interview Informant Codes of Company B

Informant Code	Position / Job Level	Department	Years of Experience
ICB01	CFO (Senior Management)	Finance	> 15 years
ICB02	Finance Manager	Finance	11–15 years
ICB03	Tax Manager	Finance	10–12 years
ICB04	Senior Finance Executive	Finance	8–10 years
ICB05	Senior Finance Executive	Finance	5–8 years
ICB06	Junior Finance Executive	Finance	3–5 years
ICB07	Junior Finance Executive	Finance	4–6 years
ICB08	Finance Assistant	Finance	2–4 years
ICB09	Finance Assistant	Finance	1–3 years
ICB10	Finance Assistant	Finance	3–5 years
ICB01	IT Manager (Senior Level)	IT	> 12 years
ICB02	IT Executive	IT	4–6 years
ICB01	HR & Admin Manager	HR	10–13 years
ICB02	Senior HR & Admin Executive	HR	6–8 years

Source: Developed for the Current Study

The following subsection further categorises these informants based on functional responsibility and scope of involvement in AIS governance.

5.4.2 Department, Role, and Job Scope Classification

The fourteen informants from Company B represent three core AIS governance domains, Finance, IT, and HR. Finance hold the largest representation, consistent with the heavy reliance on AIS for transaction postings, reporting accuracy, and audit trail maintenance. IT functions serve as system custodians overseeing cybersecurity, authentication, configuration, and access control, while HR governs payroll-related transactions and acts as the authorizing entity for system user creation and removal.

Table 5.6

Department, Role and Job Scope Classification of Company B

Department	Role Category	Job Scope Summary
Finance	Transaction & Reporting Execution	Transaction input, reconciliation, audit trails, ledger posting
IT	System Integrity & Access Control Governance	System configuration, user authentication, cyber risk oversight
Human Resource	Authorization & Compliance Administration	Payroll entries, user access approval, PDPA regulatory alignment

Source: Developed for the Current Study

The structural interplay between departments demonstrates dual accountability where Finance ensures accuracy of records while IT upholds system integrity. HR completes the governance chain through user provisioning and access authorisation controls. To complement human-based insights, organisational documents were analysed to verify policy structure, reporting flow, and approval checkpoints.

5.4.3 Document Source Codes

Documentary evidence for Company B was examined using a coded classification method, with each source assigned the prefix DCB (Document - Company B). Documents reviewed cover operational, financial, and governance areas, enabling corroboration between procedural expectations and actual user experiences expressed during interviews.

Table 5.7

Document Source Codes of Company B

Document Code	Title of Document	Issuing Department	Last Updated	Relevance to the Study
DCB01	Global AIS Reporting Manual	Parent Headquarters – Tokyo	2023	Outlines mandatory AIS procedures for all subsidiaries, forming the foundation of internal control execution in Company B.
DCB02	Finance & Authorization Matrix	Corporate Finance Department (Malaysia)	2024	Defines user access rights, approval hierarchies, financial limits, and duty segregation policies that influence control and user dilemmas.
DCB03	Cybersecurity Governance Policy	IT Security Division	2024	Regulates password cycles, access authentication, encryption requirements, and cybersecurity risk mitigation embedded in AIS.
DCB04	Monthly Financial Control Working Papers	Finance Reporting Team	2025	Provides evidence of audit trails, posting activities, month-end closing procedures and system-logged verification routines.

DCB05	HR Access Rights & Compliance Manual	HR & 2023 Compliance Department	Specifies employee data classifications, access privileges, and payroll control rules relevant to system governance and confidentiality.
-------	--------------------------------------	---------------------------------	--

Source: Developed for the Current Study

With data sources clearly defined and coded, the next Section 5.5 presents the empirical findings for Company B, beginning with an evaluation of ICG practices in its AIS environment, followed by the emergence of user challenges, operational constraints, and dilemma constructs.

5.5 ICG Practices in AIS Users of Company B

Findings from the interviews conducted with AIS users in Company B reveal that the organisation upholds a relatively structured ICG model, though with procedures that differ slightly from those implemented in Company A, reflecting both financial control requirements and the operational nature of an engineering-based organisation. Informants explained that the AIS supports not only financial reporting but also operational activities such as equipment maintenance tracking, procurement, and asset lifecycle management. As a result, governance practices are designed to ensure the protection of engineering information, operational data integrity, and system accountability.

At the organisational level, Company B establishes governance principles that guide how information is handled and protected across departments. Informants noted that controls such as **Engineering Data & Intellectual Property Protection**, **Information Classification for Technical and Financial Data**, and **Alignment with Core Organizational Value** define how sensitive engineering designs, operational records, and financial data should be managed within the AIS environment. These controls ensure that proprietary engineering knowledge, maintenance documentation, and equipment specifications remain protected from unauthorised access or disclosure. By aligning system practices with the organisation's governance principles, these mechanisms reinforce ethical behaviour, accountability, and transparency in how information is processed and shared across operational units.

In terms of access governance, Company B adopts structured mechanisms to regulate how employees and external stakeholders interact with the AIS. Controls

including **Access Authentication Requirement**, **Role-Based Engineering System Access**, **User Access Lifecycle Management**, and **Vendor & Engineering Partner System Access Control** ensure that only authorized personnel can access relevant system modules. Access permissions are granted according to job responsibilities, such as engineers, technicians, finance staff, or managers, following the principle of least privilege. Informants explained that system access must undergo approval procedures and periodic review to ensure that permissions remain appropriate throughout the employee lifecycle. External engineering vendors or equipment suppliers are also subject to restricted system access, ensuring that operational collaboration does not compromise system security or data confidentiality.

To ensure accountability in system usage and financial operations, Company B relies on monitoring and transaction control mechanisms embedded within the AIS. Controls such as **Automated Audit Trail Enforcement**, **Monitoring of System Activity**, **SoD in Operational Transactions**, and **Incident Reporting for System & Equipment Data** support transparency and traceability across operational processes. The AIS automatically logs user activities, including data entries, modifications, and approval timestamps, enabling supervisors and auditors to track operational changes and identify irregularities. Informants indicated that these automated records strengthen organisational oversight and allow internal audit functions to review system activities efficiently.

From an operational perspective, Company B also implements governance mechanisms that ensure the reliability and continuity of its integrated information systems. Controls such as **System Integration Governance**, **Technical Change Authorization**, **Secure Remote Technical Access**, and **Endpoint & Engineering Workstation Security** are designed to maintain system stability while protecting technical infrastructure. Because the AIS interacts with systems used for equipment maintenance, procurement, and asset management, changes to system configurations must undergo formal approval and testing before implementation. These measures reduce the risk of operational disruption and ensure that updates to technical systems do not compromise financial or operational data accuracy.

Data management and operational record control are also essential components of Company B's governance structure. Controls including **Equipment Lifecycle Data Control**, **Operational Data Backup & Recovery**, and **Data Retention for Equipment & Financial Records** regulate how equipment leasing information,

refurbishment history, and maintenance documentation are recorded and preserved within the AIS. Informants highlighted that these controls ensure the reliability of asset records and enable the organisation to trace the full operational lifecycle of equipment assets. Backup and recovery mechanisms further ensure that critical engineering and financial data can be restored in the event of system failures or disruptions.

From a cybersecurity perspective, Company B emphasises proactive risk management to safeguard its engineering systems and proprietary technologies. Controls such as **Vulnerability & IP Protection Controls** and **Cybersecurity Awareness** aim to mitigate cybersecurity risks while promoting responsible system usage among employees. Informants noted that employees periodically receive training and updates on cybersecurity risks related to engineering systems and digital operations. These measures help strengthen employees' awareness of system security responsibilities and reduce the likelihood of vulnerabilities arising from human error.

Despite the structured governance environment within Company B, AIS users reported that navigating these controls sometimes introduces operational challenges. Employees must comply with strict access procedures, system monitoring requirements, and documentation protocols while simultaneously managing operational workloads and meeting reporting deadlines. This situation occasionally creates tension between procedural compliance and operational efficiency, particularly when urgent operational decisions require quick system updates or approvals. Such circumstances illustrate how governance mechanisms, while necessary for accountability and system protection, may also shape the decision-making experiences of AIS users.

Table 5.8
Department, Role and Job Scope Classification

ICG Practices	Description
Engineering Data & Intellectual Property Protection	Safeguards proprietary engineering drawings, equipment specifications, maintenance algorithms, and technical documentation stored within AIS and related systems.
Access Authentication Requirement	Requires authenticated user verification before personnel can access AIS modules related to finance, procurement, equipment tracking, or maintenance records.
Alignment with Core Organizational Value	Ensures AIS practices align with the parent corporation's governance principles, including integrity in reporting, accountability, and operational transparency.
Automated Audit Trail Enforcement	Automatically records user interactions, engineering data updates, and financial transactions to ensure accountability and traceability.

Equipment Lifecycle Data Control	Governs how equipment leasing records, refurbishment history, and maintenance data are recorded, modified, and stored within AIS.
System Integration Governance	Controls the integration between AIS and operational systems such as inventory management, maintenance tracking systems, and procurement platforms.
Technical Change Authorization	Requires formal approval before updates are made to system configurations, engineering data, or equipment operational parameters recorded in AIS.
Operational Data Backup & Recovery	Ensures secure backup and recovery of engineering, operational, and financial data to maintain business continuity in the event of system failures.
Vendor & Engineering Partner System Access Control	Regulate system access granted to external engineering vendors, equipment suppliers, and maintenance contractors.
Role-Based Engineering System Access	Assigns AIS permissions according to employee roles such as engineers, technicians, finance personnel, and management.
Secure Remote Technical Access	Controls remote system access for engineers or technicians performing diagnostics, system updates, or monitoring activities.
Incident Reporting for System & Equipment Data	Establishes procedures for reporting system errors, cybersecurity incidents, or discrepancies in equipment and financial records.
Information Classification for Technical and Financial Data	Classifies sensitive data such as engineering specifications, cost structures, and equipment leasing agreements to ensure proper handling.
Monitoring of System Activity	Continuously monitors AIS activities to detect abnormal access patterns, unauthorized modifications, or unusual system behaviour.
User Access Lifecycle Management	Governs the approval, modification, and revocation of AIS access for employees, contractors, and temporary engineering staff.
Endpoint & Engineering Workstation Security	Protects engineering workstations and devices used to access AIS through antivirus protection, system hardening, and security updates.
Data Retention for Equipment & Financial Records	Defines retention requirements for engineering documentation, equipment maintenance records, and financial transaction data.
Vulnerability & IP Protection Controls	Conducts vulnerability monitoring and implements security controls to protect proprietary engineering systems and intellectual property.
Cybersecurity Awareness	Provide training to staff on cybersecurity risks related to engineering systems and AIS usage.
Segregation of Duties in Operational Transactions	Separates responsibilities across procurement, maintenance approvals, financial recording, and asset tracking to minimize manipulation risks.

Source: Developed for the Current Study

Overall, the empirical findings show that Company B maintains a clear, monitored, and structured governance environment within its AIS. These practices

demonstrate alignment with recognised governance and internal control principles while reflecting the operational needs of an engineering-focused organisation. However, similar to other governance environments, the presence of multiple and layered controls means that certain ICG practices may create operational constraints for AIS users, which are further examined in the subsequent discussion of governance-related dilemmas.

5.6 ICG Practices Creating AIS User Dilemmas of Company B

This section presents the ICG practices embedded within Company B's AIS environment and explains how these practices generate dilemmas for system users. Chapter 4 identified four ICG practices that contribute to AIS user dilemmas in Company A, namely vulnerability and IP protection controls, access authentication requirements, automated audit trail enforcement, and alignment with core organizational values. Evidence gathered from interviews and documentary sources in Company B indicates that these same practices are also present within its governance structure.

Company B operates under a dual-governance structure that combines Malaysian regulatory compliance layered with strict global reporting requirements imposed by its Japan-based headquarters. This structure results in tighter standardisation, more rigid procedures, and intensified oversight, which shape how AIS users experience ICG on daily basis. The findings from interviews and document analysis (DCB01 & DCB06) reveal that the four ICG practices also influence the operation of AIS in Company B and contribute to dilemmas experienced by users when performing their tasks. The following subsections present the empirical findings from Company B, illustrating how these practices operate within the organisation and how AIS users experience related operational challenges. The following subsections explain how each of these practices produces operational tensions and decision-making dilemmas among AIS users.

5.6.1 Vulnerability and IP Protection Controls

Company B implements strict security measures to safeguard sensitive financial and operational information within its AIS environment. Vulnerability and IP protection controls are enforced through multi-layer authentication protocols, VPN access

requirements, and restricted user permissions for sensitive system modules. These controls are designed to prevent unauthorised access, protect proprietary information, and maintain data confidentiality across the organisation.

In Company B, authentication requirements are particularly stringent due to the organisation's global reporting structure and the need to comply with security policies established by the Japan-based headquarters. Users must complete VPN login, system ID verification, and multi-level authentication before accessing certain AIS modules. In addition, password resets and new access requests require formal managerial approval.

While these measures enhance system security, AIS users reported practical challenges during daily operations. Finance staff (ICB03 & ICB07) described frequent interruptions when sessions time out or when credentials expire unexpectedly. HR administrators (ICB14) reported similar issues during payroll verification cycles when system access problems delay routine processes.

“Even simple tasks get delayed when access is stuck. We cannot proceed without IT or manager approval, and during busy periods we just wait.” (ICB03, ICB07 & ICB14 - collaborative view)

Documentary evidence (DCB05) confirms that access activation follows a multi-tier approval chain involving managerial and IT verification. Although, these controls help protect sensitive organisational information, these strict authentication protocols create operational dilemmas where users must balance compliance with the need to complete urgent operational tasks within limited timelines.

5.6.2 Access Authentication Requirements

Access authentication requirements also influence how AIS users perform their tasks in Company B. In addition to login authentication, the organisation requires strict procedural sequencing for reviewing and approving financial transactions. Sensitive activities such as payroll processing, accounting adjustments and monthly reporting entries must pass through multiple stages of verification before posting.

Finance managers (ICB02) indicated that these procedures are mandatory and must be followed according to organisational policy. As a result, users often depend on the availability of upstream reviewers before transactions can be completed. HR and Finance staff (ICB07 & ICB14) noted that even when data preparation is complete, the

process may be delayed if the designated approver is unavailable. Informants described this situation as follows:

“The review process is good for accuracy, but when deadlines are tight, the sequence becomes a bottleneck.” (ICB04, ICB05, ICB008, ICB09 & ICB010 - collaborative view)

Documentary evidence (DCB02, DCB04 and DCB05) shows mandatory two-level verification for several transaction categories. While these procedures strengthen internal control and ensure accuracy in financial reporting, they may also delay workflow completion when operational deadlines are approaching.

5.6.3 Automated Audit Trail Enforcement

Automated audit trail enforcement is another governance practice observed in Company B’s AIS environment. Similar to many enterprise accounting systems, the AIS records user activities including data entry, transaction modifications, approval actions, and system access logs. This functionality allows management and internal auditors to review system activities and trace transactions when discrepancies occur.

In Company B, system permissions are tightly controlled to prevent unauthorised changes and cross-subsidiary data exposure. As a result, several system functions are restricted to authorised personnel, and AIS users frequently rely on IT staff to resolve system issues. Examples of tasks that typically require IT support include:

- (a) error log clearance.
- (b) module reactivation.
- (c) access reinstatement.
- (d) resolving authentication failures.
- (e) configuration of standard reports.

IT staff (ICB11 and ICB12) confirmed that system permissions are intentionally limited to maintain control over system operations and protect sensitive organisational data. As explained by informants:

“Many functions are locked by design. Users cannot troubleshoot. Everything must go through IT for safety reasons.” (ICB04, ICB05, ICB06, ICB07, ICB08, ICB010 and ICB014 - collaborative view)

While these system controls support monitoring and accountability, this creates structural dependency, leaving AIS users stuck when IT response times do not align with peak cycles such as month-end closing. The resulting dilemma stems from conflicting expectations: users must complete tasks promptly, yet the system prevents them from resolving issues independently.

5.6.4 Alignment With Core Organizational Values

Alignment with core organisational values also shapes the way AIS users perform their responsibilities in Company B. The organisation emphasises integrity, transparency and accuracy in financial reporting, and these values are reinforced through system validation procedures, mandatory verification steps, and clearly defined reporting timelines.

Company B operates within a global corporate structure where the Japan-based headquarters requires strict compliance with financial reporting standards. Financial schedules must be completed accurately and submitted according to specific deadlines before consolidation at headquarters. Finance executives (ICB04 and ICB05) reported that these reporting requirements create pressure on AIS users to ensure both accuracy and timeliness in their work. Informants noted:

“The dilemma is whether to follow every step and risk missing deadlines or move faster and risk being questioned later.” (ICB02, ICB05, ICB009 and ICB010 - collaborative view)

Documentary data (DCB03) confirms financial submissions must meet strict validation requirements before headquarters consolidation. While these procedures support organisational values and strengthen financial accountability, they also increase workload pressure for AIS users who must balance speed and precision during reporting periods. These conditions create dilemmas between operational urgency and the requirement to maintain strict data quality standards.

Table 5.9

Summary of ICG Practices Creating Dilemmas for AIS Users in Company B

ICG Practices	Observed Implementation in Company B	Supporting Evidence
Vulnerability and IP Protection Controls	Multi-layer authentication, VPN access, and restricted system permissions	ICB03, ICB07, ICB14, DCB05
Access Authentication Requirements	Sequential approval procedures and mandatory transaction verification	ICB02, ICB04, ICB07, ICB14, DCB02
Automated Audit Trail Enforcement	System monitoring and restricted permissions requiring IT intervention	ICB04, ICB05, ICB06, ICB11, ICB12
Alignment with Core Organizational Values	Strict reporting deadlines and validation requirements from headquarters	ICB02, ICB05, ICB09, DCB03

Source: Developed for the Current Study

The findings presented in this section show that the four ICG practices identified in Chapter 4 are also present within Company B's AIS environment. Evidence from interviews and documentary sources demonstrates how these practices operate in the organisation and how AIS users experience related operational challenges when performing their daily responsibilities. The next section further examines the broader conditions that contribute to the dilemmas encountered by AIS users within Company B's governance and operational environment.

5.7 Dilemmas Experienced by AIS Users in Relation to ICG Practices of Company B

The empirical findings revealed that AIS users in Company B encounter dilemmas that arise not from a single isolated cause, but from the combined influence of several interrelated governance, technical and operational occurrences embedded within the AIS environment. While ICG practices aim to safeguard accuracy, enforce accountability and strengthen system reliability, these same mechanisms also generate constraints, interruptions, and practical tensions in daily work. Analysis of the interview data indicates that the five recurring themes identified in Company A are also applicable to Company B. However, the AIS environment in Company B, which integrates strict global reporting requirements and higher technical controls, shapes how these dilemmas are experienced by AIS users. Five dominant influences emerged consistently across the fourteen informants that include (a) regulatory compliance pressure, (b) cybersecurity control restriction, (c) ethical tension, (d) bureaucratic procedures from SoD, and (e) technology-related performance anxiety. The subsections below present

each dilemma experienced by AIS users supported by explanation and interview extracts.

5.7.1 Regulatory Compliance Pressure

Company B enforces rigorous authentication procedures involving VPN login, system-generated IDs, and multi-layer verification for sensitive tasks. While these controls enhance security, many users expressed that the strictness of these protocols creates operational tensions. Resetting credentials requires senior-level approval, and delays are common during peak periods. Informants described these situations:

“Even small tasks become stuck when access expires, or the system logs us out for security. We cannot proceed unless IT approves the reset, and this slows down our entire process.” (ICB06, ICB07, ICB08 and ICB010 - collaborative view)

“Sometimes routine work comes to a halt because the system blocks certain functions without warning. We must wait for the IT team to verify and unlock the access, and this delay affects not just our tasks but everyone who depends on our input.” (ICA03, ICA10 and ICA14 - collaborative view)

These examples illustrate how the strict compliance culture, though necessary, introduces dilemmas when users must balance governance adherence with timely task completion.

5.7.2 Cybersecurity Control Restriction

ICG structures in Company B emphasise stringent approval hierarchies to protect data integrity. However, this rigidity often results in bottlenecks, especially when multiple approvals are required for routine postings or corrections.

“The procedures are very rigid. Small adjustments need several levels of approval. We understand the rationale, but it becomes a dilemma when deadlines are tight and approvals are stuck.” (ICA07, ICA09 & ICA10 - collaborative view)

“We get why the controls are there, but honestly, even simple tweaks end up going through so many layers. We try to follow the steps, but it is tough when urgent work gets held up just because the approvals are not moving.” (ICB05, ICB08 & ICB14 - collaborative view)

AIS users experience dilemmas as they are caught between adhering with cybersecurity protocols while facing operational delay, resulting in recurring tensions.

5.7.3 Ethical Tension

Ethical considerations present a complex challenge for AIS users operating under ICG. While the ethical standards of a profession and the personal values of ethicists may align, they often diverge from the corporate culture and operational procedures mandated by the organization. Professional ethics require strict adherence to codes of conduct that emphasize transparency, fairness, and integrity in the execution of financial and operational tasks. However, organizational structures may impose operational constraints that limit the full application of these ethical principles, particularly in highly regulated or proprietary environments.

At Company B, ethical practice is shaped not only by professional standards but also by corporate protocols designed to protect IP, ensure data confidentiality, and promote commercial competitiveness. This tension can result in ethical dilemmas for AIS users who must balance their professional obligations with organizational expectations. For instance, staff may encounter situations where regulatory compliance or task efficiency conflicts with personal or professional ethical judgments. These dilemmas become more acute when ethical rigidity impedes collaboration or delays task completion. Employees deeply committed to professional ethics referred to here as ethicists and may be unwilling or unable to compromise their values to align with organizational norms. As a result, their strict adherence to ethical codes, though well-intentioned, can hinder workflows and affect interpersonal dynamics in the workplace. This was highlighted by several informants who noted:

“AIS are intricately linked to various financial and operational functions within an organization, playing a critical role in maintaining efficiency, accuracy, and competitiveness in the business environment. Given this significant role, the operation of AIS must consistently align with established ethical standards in accounting. Every decision or action taken within the system whether related to data entry, reporting, or internal control can have far-reaching implications, not only for the organization’s performance but also for the welfare of stakeholders, including employees, clients, and regulatory bodies. As such, ethical compliance is not optional, but it is a fundamental expectation that ensures trust, accountability, and the integrity of financial information under regulatory scrutiny.” (ICB04, ICB05, ICB06, ICB07, ICB08, ICB09, ICB10 and ICB14 - collaborative view)

Several informants further emphasized the human element of ethical practice that *“Ethics are what keep the profession grounded as they ensure fairness in practice and maintain the public’s trust in accountants. In our line of work, especially when dealing with financial data through an AIS, ethical judgment must always be at the core. The system might automate transactions and standardize processes, but at the end of the day, it is people who make decisions, interpret data, and approve actions. We cannot expect accountants to operate like robots and purely based on programmed logic. They are human beings, and that human element is critical. With all the pressure to meet deadlines, satisfy stakeholders, and work efficiently within digital systems, the temptation to override controls or bend the rules can arise. That is why ethical awareness and accountability are more important than ever. An ethical lapse in judgment, especially in a computer-based AIS, can go unnoticed until considerable damage is done. So, ethics is not just about compliance, but it is about professional integrity, responsibility, and doing what is right, even when no one is watching”* (ICB01, ICB03, ICB07, ICB11 and ICB13 - collaborative view)

These observations illustrate how the human aspect of ethics concern for fairness, flexibility, and moral judgment and must coexist with the procedural demands of AIS. When organizational rules are rigid and narrowly defined, ethicists may struggle to adapt, which can lead to tension within teams or delays in decision-making. This challenge was also noted by a finance manager, who stated an ethicist is so consumed that he or she finds it difficult to shift ground in relation to certain standard rules and regulation that is considered inherent to the ethics he or she has gone along way with. When an ethicist is unable to adjust to the standard, the co-workers or other are affected by the tight impose disposition to adhere to the ethics. Most ethicist finds themselves in another dilemma of how to please others or adhere to the rules, regulation, and ethics of the profession. Should ethicist adamantly adhere or stick to an uncompromised disposition in each organization, every other person that work with them will suffer harsh working relationship. This tight, rigorous, and impracticable ethicist behaviour will detail every task that will in turns put a burden of duty on others. As explained by informants:

“AIS are not merely tools for processing financial transactions; they fundamentally reflect human intentions and decision-making. Behind every entry and report, there are people whose values, ethics, and judgments influence how information is recorded and used. Therefore, AIS cannot be viewed purely as technical systems, they

are intertwined with the human element, where intentions, whether ethical or otherwise, shape the outcome of the data. Recognizing this helps us understand why strong internal controls and ethical frameworks are essential to ensure that AIS operate not only efficiently but also with integrity.” (ICB02, ICB03, ICB05, ICB08, ICB09 and ICB13 - collaborative view)

This perspective reinforces the notion that ethical dilemmas in AIS are not purely technical but are influenced by human judgment, values, and interdependent workflows. Consequently, ethical issues within ICG frameworks highlight the need for balance between maintaining high ethical standards and enabling efficient, collaborative decision-making in complex organizational settings.

5.7.4 Bureaucratic Procedures from Segregation of Duties

AIS users in Company B carry dual expectations, they must maintain high data accuracy while also meeting strict reporting deadlines. This dual expectation is a major source of pressure, and users often struggle to balance accuracy with speed, especially when the system enforces numerous validation checks. Informants described:

“The procedures are very rigid. Small adjustments need several levels of approval. We understand the rationale, but it becomes a dilemma when deadlines are tight and approvals are stuck.” (ICB04, ICB05, ICB06 and ICB07 - collaborative view)

“We try to follow all steps, but urgent work often gets held up because approvals aren’t moving.” (ICA02, ICA03 and ICA08 - collaborative view)

These occurrences illustrate how SoD, although designed to maintain control, introduces dilemmas when speed and flexibility are required.

5.7.5 Technology-Related Performance Anxiety

Although Company B has established group-wide policies, the interpretation of these rules varies across departments, particularly between Finance, IT and HR. Automated validations, error logs, and cross-department coordination increase workload pressure. Different departments interpret governance rules differently, creating confusion and duplicated efforts. Informants explained:

“Each department views the control rules differently. Finance wants more flexibility, IT wants more restrictions, and HR focuses on confidentiality. Sometimes we are not aligned.” (ICB01, ICB03 & ICB13 - collaborative view)

“Every team seems to have its own take on the control requirements. Finance pushes for faster processing, IT prioritizes system security, and Procurement just wants fewer steps. So sometimes we end up misaligned without realising it.” (ICB02, ICB04 & ICB11 - collaborative view)

These occurrences reveal how system complexity and departmental variations induce performance anxiety and dilemmas for AIS users, especially in tasks involving cross-department collaboration or multi-system workflows.

The findings in Company B demonstrate that the dilemmas identified in Company A also occur in a different organizational and technological context. While the operational and technical environment in Company B is more complex and control-intensive, the themes remain consistent. The dilemmas described above illustrate how AIS users navigate governance compliance, system restrictions, and operational demands in their daily work. The next section examines how users mitigate these dilemmas and the strategies they adopt to maintain compliance while achieving operational efficiency.

Table 5.10
Summary of Dilemmas Experienced by AIS Users in Relation to ICG Practices of Company B

Theme	Description of Dilemma Experienced	Supporting Informants
Regulatory Compliance Pressure	Strict authentication procedures, system access controls, and approval requirements interrupt workflow and delay task completion when users must wait for authorization to proceed.	ICB06, ICB07, ICB08, ICB10, ICB03, ICB14
Cybersecurity Monitoring Restrictions	Rigid cybersecurity monitoring and layered approval hierarchies create operational bottlenecks when routine corrections or postings require multiple levels of authorization.	ICB05, ICB07, ICB08, ICB09, ICB10, ICB14
Ethical Tension	AIS users experience ethical tension when professional ethical standards and personal moral judgment must be balanced with organizational procedures, system constraints, and operational expectations.	ICB01, ICB02, ICB03, ICB04, ICB05, ICB06, ICB07, ICB08, ICB09, ICB10, ICB11, ICB13, ICB14
Bureaucratic Procedures from Segregation of Duties	SoD and multi-level approval processes increase procedural complexity, causing delays when urgent transactions or adjustments require several approvals.	ICB04, ICB05, ICB06, ICB07, ICB02, ICB03, ICB08
Technology-Related Performance Anxiety	System complexity, automated validations, and inconsistent rule interpretation across departments increase workload pressure and create uncertainty during cross-department collaboration.	ICB01, ICB02, ICB03, ICB04, ICB11, ICB13

Source: Developed for the Current Study

The findings in Company B demonstrate that the dilemmas identified in Company A also occur in a different organizational and technological context. While the operational and technical environment in Company B is more complex and control-intensive, the themes remain consistent. The dilemmas described above illustrate how AIS users navigate governance compliance, system restrictions, and operational demands in their daily work. The next section examines how users mitigate these dilemmas and the strategies they adopt to maintain compliance while achieving operational efficiency.

5.8 Mitigating AIS User Dilemmas Related to ICG of Company B

The empirical findings from Company B show that AIS users do not simply follow internal control requirements; rather, they actively negotiate, adjust, and improvise their work practices to cope with the dilemmas created by ICG mechanisms. These coping strategies are not random actions but are formed patterns shaped by organisational rules, system constraints, and cross-department expectations. When compared with the broader behavioural themes identified in Company A's regulatory awareness, obligation and process, corporate culture, reporting standards, and productivity and performance, it becomes clear that these original themes manifest differently in Company B due to its stronger security emphasis, highly structured approval workflow, and heavier IT dependency. As such, five mitigation strategies emerged from the interviews, observation records, and document review conducted in Company B:

- (a) regulatory awareness
- (b) procedural compliance
- (c) corporate culture alignment
- (d) reporting discipline, and
- (e) productivity and performance adaptation

These coping strategies illustrate how AIS users navigate conflicting demands between compliance and operational practicality.

5.8.1 Regulatory Awareness

AIS users employ various adaptive behaviours to handle frequent logouts, password expirations, and multi-step verification requirements. Many plan tasks around peak-hour disruptions or pre-emptively refresh credentials to avoid downtime.

“Before month-end closing, I always reset my password earlier because if it expires during closing, we cannot do anything until IT approves the reset.” (ICB04, ICB05, ICB07 and ICB10 - collaborative view)

“We learn to expect delays. Sometimes we log in earlier or do drafts offline so we can upload immediately when the system finally allows access.” (ICB03, ICB08 and ICB14 - collaborative view)

These responses demonstrate how users internalize security constraints and develop anticipatory routines to continue functioning despite authentication barriers.

5.8.2 Procedural Compliance

Users develop tactical approaches to navigate the multi-level approval processes that slow down routine entries, adjustments, or corrections. These coping strategies include early submission, negotiation with approvers, and informal follow-ups.

“If we know that three approvals are needed, we submit everything a day earlier. Otherwise, our work gets stuck, especially if one of the approvers is not available.” (ICB06, ICB08 and ICB14 - collaborative view)

“Sometimes we remind the approvers personally, not because we want to skip the process but because the timeline is too tight.” (ICB07, ICB09 and ICB10 - collaborative view)

These behaviours show how users compensate for procedural rigidity by strategically coordinating approvals to meet operational deadlines.

5.8.3 Corporate Culture Alignment

The corporate culture in Company B is influenced by strong emphasis on operational discipline through centralized control and system governance. According to many Informants explanations, many AIS procedures and system configurations are administered by policies and standards. These policies are thoughtfully determined either by headquarters or by the central technical governance units of the organization.

This structure requires all employees to strictly follow established processes whenever they are interacting with the AIS tool. This centralized approach reinforces organizational consistency through a unified control across board. Nonetheless, it also requires users to continuously adjust their work practices to comply with all system restrictions and formal operational protocols.

The uniformity of all informants' justification highlights the discipline of procedural culture that encourages employees to prioritize both rules of engagement, system compliance, and adherence to formal processes. Rather than bypassing restrictions and protocol, users tend to align approval, validations, documentation requirements as well as rules and regulation into their everyday routines. This process further denotes the flow of governance structure that shapes not only the technical procedure but also extends to employees' perception of their daily task and responsibilities. An IT executive acknowledged that the existence of strict system controls is intentionally designed to safeguard and maintain governance standards. An IT executive acknowledged:

"We lock many features for security. So yes, users need us for things like reactivating access or unlocking transactions." (ICB12)

Finance personnel explained that this centralized system control directly influences and shapes how they plan and organize their daily tasks. Since certain system actions require intervention or validation from the IT function, users are expected to structure their work schedules around these checkpoints accordingly. As described by finance staff member:

"We schedule our tasks based on when IT is available. If IT is slow, we move to other tasks first." (ICB02, ICB04 and ICB09 - collaborative view)

These responses suggest that AIS users cope with the centralized governance structure by adapting their workflow to align with system procedures and departmental coordination. Instead of challenging the restrictions imposed by the system, users prioritize procedural correctness and compliance with governance standards established by the organization. Such behaviour reflects an organizational culture that values control, reliability, and consistency across operational processes.

While this disciplined governance environment supports accountability and system integrity, informants acknowledged that it also requires flexibility in how tasks are managed. Users frequently adjust their working patterns, coordinate with technical teams, and reorganize priorities to ensure that operational activities remain aligned with

system requirements. This demonstrates how corporate culture in Company B shapes user behaviour by encouraging adherence to centralized operational discipline while maintaining coordination across functional and technical departments.

5.8.4 Reporting Discipline

AIS users manage the tension between accuracy and reporting deadlines by sequencing tasks, double-checking critical entries, and prioritising high-risk data fields. As describe by informants from finance department:

“We cannot afford mistakes because the system will flag them, and corrections take time. So, we pace the workload carefully.” (ICB01, ICB04 and ICB05 - collaborative view)

Other informants added:

“At closing, we work late not because of the volume alone but because every detail must follow the control steps.” (ICB02, ICB06, ICB08, ICB09 and ICB10 - collaborative view)

These coping behaviours demonstrate how users strive to maintain both accuracy and timeliness, even under restrictive controls that impede data processing efficiency.

5.8.5 Productivity and Performance Adaptation

Users respond to differing departmental interpretations of rules by seeking clarifications, escalating uncertainties, or aligning with the most conservative interpretation to avoid non-compliance.

“Finance sees controls differently from IT. Sometimes the rule means one thing to them and another to us. We usually clarify with email, so everyone agrees.” (ICB13)

“Each department protects its own area. So, we often negotiate what is acceptable before proceeding.” (ICB02, ICB03, ICB05 and ICB14 - collaborative view)

These behaviours indicate that coping involves relational work, negotiation, clarification, and alignment rather than individual action alone.

Table 5.11

Summary on Mitigating AIS User Dilemmas Related to ICG of Company B

Mitigation Strategy	Description of Coping Behaviour	Supporting Informants
Regulatory Awareness	AIS users anticipate authentication barriers by resetting credentials earlier, logging in ahead of peak periods, and preparing draft work offline to avoid disruptions caused by system security controls.	ICB03, ICB04, ICB05, ICB07, ICB08, ICB10 & ICB14
Procedural Compliance	Users navigate multi-level approval processes by submitting tasks earlier, coordinating with approvers, and conducting informal follow-ups to prevent workflow delays.	ICB06, ICB07, ICB08, ICB09, ICB10 & ICB14
Corporate Culture Alignment	AIS users adapt their workflow to align with centralized governance structures by scheduling tasks around IT availability and adhering closely to system procedures and approval protocols.	ICB02, ICB04, ICB09 & ICB12
Reporting Discipline	Users manage the pressure between accuracy and deadlines by pacing workloads, prioritizing critical entries, and carefully sequencing reporting tasks to comply with system validations.	ICB01, ICB02, ICB04, ICB05, ICB06, ICB08, ICB09 & ICB10
Productivity and Performance Adaptation	AIS users mitigate cross-department governance differences by seeking clarification, negotiating acceptable interpretations, and aligning with the most conservative rule application to avoid compliance risks.	ICB02, ICB03, ICB05, ICB13 & ICB14

Source: Developed for the Current Study

The findings in Company B demonstrate that AIS users do not passively accept the operational constraints created by internal control governance mechanisms. Instead, they develop adaptive work practices to mitigate the dilemmas encountered in their daily interactions with the AIS environment. As summarised in Table 5.11, these mitigation strategies include anticipating authentication disruptions, coordinating approval processes, aligning with centralized governance expectations, carefully managing reporting workloads, and negotiating cross-department interpretations of governance rules.

These coping behaviours illustrate that AIS users continuously balance compliance obligations with operational practicality. While strict governance controls strengthen system integrity, they also require users to adjust their routines, coordinate with technical teams, and strategically organize their work activities to maintain productivity. Through these adaptive responses, AIS users are able to sustain operational continuity while remaining within the boundaries of the organization's control framework.

Overall, the findings highlight that mitigating AIS-related dilemmas is not solely a technical process but also a behavioural and organizational response shaped by governance structures, system constraints, and collaborative interactions across departments.

5.9 Chapter Summary

This chapter provides an in-depth analysis of the case study for Company B, with a particular focus on the internal control mechanisms as they pertain to the dilemmas faced by AIS users within the organization. It offers a comprehensive explanation of the specific internal control processes implemented and examines how these controls interact with the practical challenges encountered by AIS users on daily basis. The chapter systematically investigates a range of factors that contribute to these dilemmas, including technological, procedural, and human elements, thereby providing a nuanced understanding of the root causes and complexities involved.

In addition, the chapter describes the operational impacts of these dilemmas on AIS users' work practices, highlighting how internal control requirements may lead to operational delays, additional coordination efforts, or increased compliance responsibilities. The chapter draws on empirical evidence from interviews, observations, and document reviews conducted in Company B to present a detailed case account of how internal control governance operates in practice.

The following chapter expands the discussion by comparing the dilemmas faced by AIS users in Company A and Company B. It highlights similarities and differences in internal control and CG challenges and examines the connection between AIS controls and broader governance mechanisms. The chapter concludes with a synthesis of findings, a critical review of relevant literature, and recommendations to improve ICG and AIS user performance in the Malaysian corporate context.

CHAPTER 6

FINDING AND DISCUSSION

6.1 Introduction

The cross-case analysis presented in this chapter are empirical findings obtained from both case study of Company A listed in Chapter 4 and case study of Company B listed in Chapter 5 above. The primary goal of this chapter is to synthesize similarities and differences in AIS users' experiences as it relates to ICG practices embedded within AIS environments (Yin, 2020). The entire process is guided by a thematic analysis approach (Braun & Clarke, 2016; Nowell et al., 2017) which is predicated on Trade Off Theory (March & Simon, 1958; Imdieke et al., 2023; Nguyen & Lee, 2024). This chapter systematically discourses the three core research objectives by examining how ICG related dilemmas emerge, how they affect AIS users' decision-making and workload performance, and how users attempt to balance governance requirements with operational efficiency (Hussain et al., 2023; Othman et al., 2023).

Contrasting the in-case analyses earlier presented in both chapter 4 and 5 above, chapter 6 moves beyond contextualising individual organisational to identify cross-case patterns, strengthening the study's explanatory power and reinforcing analytical generalisation (Yin, 2020).

6.2 Overview of Cross Case Analytical Approach

This study employed a cross-case thematic analysis for comparing and contrasting the empirical findings emanating from both Company A and Company B (Yin, 2020; Nowell et al., 2017). The adoption of cross-case approach was to inch further from mere organisation-specific descriptions to identifying patterns of convergence and divergence on how ICG practices embedded within AIS are experienced by users across diverse organisational settings (Hussain et al., 2023; Wang & Chen, 2021). This study strengthens analytical generalisation and enhances the robustness of the findings by analysing both cases in parallel (Yin, 2020).

The initial themes developed using in-case analysis in Chapters 4 and 5 were re-scrutinized diligently with higher level of abstraction (Braun & Clarke, 2016; Nowell et al., 2017). This process involved the comparison of how similar ICG practices

manifested across the two organisations in study, assessing whether AIS user dilemmas consistently emerged or varied due to governance structure, differences in system configuration, or organisational context (Wang & Chen, 2021; Hussain et al., 2023). Researchers focused more on uncovering mechanisms that repeatedly create or lead to dilemmas, by examining their collective effects on decision-making and workload, and exploring predictable coping methods used by AIS users (Ibrahim et al., 2024; Othman et al., 2023).

The trajectory of the cross-case analysis followed a theory-informed interpretive logic, rather than a purely descriptive comparison (Yin, 2020). Trade-Off Theory was employed as the primary analytical lens to interpret how AIS users navigate conflicting organisational demands (March & Simon, 1958; Imdieke et al., 2023; Nguyen & Lee, 2024). Unambiguously, this theory was used to elucidate how users balance compliance-based ICG controls such as SoD, approval hierarchies, access restrictions, and audit requirements; as against the need for timely completion of task, operational flexibility, and performance efficiency (COSO, 2013; ISACA, 2022; Kassem et al., 2023; Almeida et al., 2023). The theoretical framing enabled this study to conceptualise AIS user dilemmas not merely as isolated operational problems, rather as outcomes of structural trade-offs embedded within governance-controlled system (March & Simon, 1958; Nguyen & Lee, 2024).

Beyond this approach, the cross-case analysis addressed the three core research objectives in an all-incorporated method. First, it enabled the identification of ICG practices embedded in AIS that consistently create dilemmas for users across subsidiaries of the organization in study (Hussain et al., 2023; Wang & Chen, 2021). Second, it facilitated the examination of how these dilemmas influence AIS users' decision-making and workload performance, further highlighting both cognitive and operational effects (Othman et al., 2023; Nordin & Yeoh, 2024). Third, it supported exploration of strategies AIS users engage to balance ICG requirements with operational efficiency, thus, revealing adaptive behaviours that emerge in response to governance constraints (Ibrahim et al., 2024; Yusof & Basir, 2021).

The overall concept of the cross-case analytical approach ensured that Chapter 6 functions as a synthetic and explanatory chapter. Thus, it aims at bridging the findings from individual cases with the broader theoretical discussion while preparing the foundation for the study's contributions and implications presented in subsequent chapters (Yin, 2020).

6.3 Cross Case Analysis by Research Objectives

At this stage, a progressive approach combines evidential findings from Company A and Company B to form a unified understanding of how ICG is reflected in routine AIS operations. Through the comparison of collective patterns and contrasting practices in both cases, the analysis demonstrates how control-governance can be viewed either as constructive safeguards or as limiting constraints on operations. The cross-company comparison therefore strengthens the credibility of the refined themes by proving how similar dilemmas arise under diverse organisational settings, while also revealing context-specific variations in interpretation, work pressure, and user coping responses.

6.3.1 RO1: ICG Practices Embedded in AIS That Create Dilemmas for Users

Both Company A and Company B supporting evidence confirms that ICG practices embedded within AIS aims at strengthening control, accountability, and compliance (COSO, 2013; ISACA, 2022; Hussein et al., 2023). Conversely, these practices repeatedly give rise to user dilemmas when operational realities conflict with rigid controls (March & Simon, 1958; Imdieke et al., 2023; Nguyen & Lee, 2024). While Chapters 4 and 5 identified detailed ICG practices embedded within AIS, the themes presented in Section 6.3.1 do not restate those practices. As an alternative, they represent cross-case analytical interpretations of how these controls are experienced, performed, and navigated by AIS users in daily work (Braun & Clarke, 2016; Nowell et al., 2017). The shift from named control practices to experiential themes reflects the move from descriptive within case findings to higher level cross-case abstraction (Yin, 2020).

Key Cross Case Themes Identified:

- (a)** Rigid approval hierarchies (Almeida et al., 2023; Karim & Fathil, 2023)
- (b)** SoD embedded in system workflows (Nguyen et al., 2020; Kassem et al., 2023; Yap & Cheong, 2024)
- (c)** Restricted system access and role-based permissions (Ahmad Zazili et al., 2024; Khalid & Othman, 2024; Kassem et al., 2024)
- (d)** Standardised reporting formats with limited flexibility (Rahman et al., 2023; Nordin et al., 2023)

In both cases, AIS users reported difficulties when system embedded controls constrained their ability to respond promptly to operational demands, as highlighted by informants, consistent with evidence that embedded controls can generate process friction and user-level constraints in governed AIS environments (Hussain et al., 2023; Wang & Chen, 2021). While Company A emphasised formal compliance and documentation discipline, Company B highlighted challenges arising from centralised control structures imposed across multiple subsidiaries, as highlighted by informants (Lopez & Garcia, 2021; Chen et al., 2020).

Table 6.1
RO1: Cross-Case Triangulation of ICG Practices Creating AIS User Dilemmas

ICG Practices	Cross-Case Insight	Evidence: Company A	Evidence: Company B	Supporting Documents	Prior Case Studies Supporting This Pattern
Vulnerability & Protection Controls	Stringent security controls (timeouts, VPN, multi-layer authentication) create workflow interruptions and delays, generating user dilemmas between compliance vs task completion.	ICA03, ICA07, ICA10, ICA14	ICB03, ICB14	ICB07, DCA02, DCA05; DCB05	Spears & Barki (2010) show cybersecurity controls frequently obstruct business workflow; Sverdlik (2012) shows authentication friction creates user dilemma.
Access Authentication Requirements	Mandatory sequential approvals slow task progression; users experience bottlenecks dependent on approved availability.	ICA04, ICA05, ICA08, ICA09	ICB02, ICB07, ICB14	ICB04, DCA03; DCB02, DCB04	Kottemann & Konsynski (2011) identify approval chains as structural bottlenecks; Kim et al. (2009) show authentication rules cause procedural congestion.
Automated Audit Trail Enforcement	System-imposed restrictions increase dependency on IT, creating dilemmas when users must choose between waiting for IT or missing deadlines.	ICA06, ICA08, ICA10	ICB04, ICB06, ICB12	ICB05, DCA03; DCB05	Masrek & Jusoff (2009) confirm audit-trail rigidity increases IT reliance; Silva & Hirschheim (2007) emphasise tensions from system immutability.

Alignment with Organisational Values	Pressure to meet accuracy + timeliness creates dilemma between following full compliance steps vs ensuring reporting deadlines.	ICA02, ICA09	ICA05,	ICB02, ICB10	ICB05,	DCA01, DCA04; DCB03	Ghosh et al. (2011) show strong corporate values increase ethical/operational tension; Trotman et al. (2015) confirm accuracy–speed trade-off in AIS.
---	---	-----------------	--------	-----------------	--------	------------------------	---

Source: Developed for the Current Study

These findings indicate that while ICG practices are structurally necessary, their system embedded nature transforms governance mechanisms into sources of operational tension (Brown & Adams, 2023; Martinez & Clark, 2024; Hussain et al., 2023).

6.3.2 RO2: User's Dilemma Towards ICG Practices Embedded in AIS

Across both organisations, ICG related dilemmas were found to directly influence AIS users' decision-making processes and workload distribution, as highlighted by informants, consistent with literature linking internal control burden to performance strain (Othman et al., 2023) and compliance-first behaviour in reporting systems (Nordin & Yeoh, 2024). Users frequently faced trade-offs between adhering strictly to system controls and meeting operational timelines (March & Simon, 1958; Imdieke et al., 2023; Nguyen & Lee, 2024). These trade-offs were not merely procedural but cognitive and behavioural, as users continuously reassessed risk, responsibility, and timing when executing AIS related tasks (Thomas & Khalid, 2023; Nordin & Yeoh, 2024).

As a result, decision making became increasingly conservative and workload intensive, with users prioritising error avoidance and audit defensibility over speed or task optimisation, as highlighted by informants, consistent with research on traceability pressure and defensive user behaviour in digital accounting systems (Cheng & Abdullah, 2023; El-Shafey & Omar, 2024; Gordon, 2023).

Cross Case Effects Identified:

- (a)** Increased cognitive load due to work-around decision making (Thomas & Khalid, 2023; Nordin & Yeoh, 2024)
- (b)** Delayed decision approvals (Almeida et al., 2023; Karim & Fathil, 2023)
- (c)** Duplication of effort outside AIS (Ibrahim et al., 2024; Yusof & Basir, 2021)
- (d)** Increased reliance on informal controls (Ibrahim et al., 2024; Ibrahim et al., 2023)

AIS users in Company A reported heightened workload pressures during peak reporting periods due to system constraints, whereas users in Company B highlighted decision delays caused by group level approvals and limited local discretion, as highlighted by informants, aligning with findings on centralised governance constraints in multinational structures (Lopez & Garcia, 2021; Chen et al., 2020; Wang & Chen, 2021).

Table 6.2

RO2: Cross-Case Triangulation of AIS User Dilemmas

Dilemma Theme	Cross-Case Insight	Evidence: Company A		Evidence: Company B		Published Case Studies Supporting This Pattern
Regulatory Compliance Pressure	Users must comply with strict controls but face operational delays, creating dilemma between governance compliance & workflow continuity.	ICA03, ICA14	ICA10,	ICB06, ICB08, ICB10	ICB07,	Spears & Barki (2010) demonstrate governance-security friction; Al-Momani (2016) shows compliance-induced workflow constraints.
Cybersecurity Monitoring Restrictions	Multiple approval layers and locked system features cause bureaucratic bottlenecks.	ICA07, ICA10	ICA09,	ICB05, ICB14	ICB08,	Kottemann & Konsynski (2011) describe multi-level approval delays; Vance et al. (2012) confirm user stress from monitored systems.
Ethical Tension	Users struggle balancing personal/professional ethics with organisational efficiency and system constraints.	ICA01, ICA06	ICA05,	ICB01–ICB14 (broad coverage)		Ghosh et al. (2011) explain ethical vs organisational mandate conflict; Sarker et al. (2019) show ethics become a site of dilemma in procedural systems.
Bureaucracy Segregation from Duties	Soda rules cause multi-step delays when approvers are unavailable.	ICA02, ICA08	ICA03,	ICB04, ICB06, ICB07	ICB05,	Weill & Ross (2004) show Soda increases structural delays; Bowen et al. (2009) confirm SoD–speed trade-off in AIS workflows.
Technology-Related Performance Anxiety	System errors, validations, and cross-department rule incoherence cause anxiety and duplicated work.	ICA01, ICA08	ICA04,	ICB01, ICB11, ICB13	ICB03,	Tarafdar et al. (2015) describe “technostress” from system controls; Kaganer et al. (2010) link AIS complexity to user anxiety.

Source: Developed for the Current Study

The findings suggest that AIS users do not merely experience inconvenience but actively re allocate effort to manage governance induced constraints, as highlighted by informants, consistent with empirical work on governance intensity and workflow backlog in regulated AIS environments (Ibrahim et al., 2023; Hussain et al., 2023).

6.3.3 RO3: Strategies for Balancing ICG Practices While Mitigating Operational Efficiency in AIS

Across both cases, three final, integrated themes emerged. These strategies reflect adaptive user behaviours aimed at preserving task completion and accountability under ICG constraints, thereby making the control efficiency trade-off manageable in day-to-day AIS use.

Theme: User Interpretation of ICG as Situated Sensemaking

Despite these challenges, AIS users in both organisations demonstrated adaptive strategies to balance governance compliance with operational efficiency, as highlighted by informants, consistent with research on informal workarounds under digital control constraints (Ibrahim et al., 2024) and unintended consequences of governance on AIS usability (Yusof & Basir, 2021). These strategies reflect practical trade-offs rather than formal system redesign (March & Simon, 1958; Nguyen & Lee, 2024). Rather than resisting or bypassing controls, users engaged in adaptive work practices such as task sequencing, advance coordination of approvals, and selective prioritisation of high-risk activities, as highlighted by informants (Ibrahim et al., 2024; Nur & Yusoff, 2024).

These strategies enabled users to preserve operational flow while remaining compliant, demonstrating that coping under ICG is enacted through behavioural adjustment rather than structural change (Hussain et al., 2023; Ibrahim et al., 2024).

Cross Case Balancing Strategies:

- (a) Informal pre-approvals before system submission (Karim & Fathil, 2023; Ibrahim et al., 2024)
- (b) Parallel offline tracking to supplement AIS limitations (Yusof & Basir, 2021; Ibrahim et al., 2024)
- (c) Role stretching during peak periods (Othman et al., 2023; Nur & Yusoff, 2024)
- (d) Selective prioritisation of compliance versus timeliness (March & Simon, 1958; Indieke et al., 2023; Nguyen & Lee, 2024).

Table 6.3

RO3: Triangulation of Mitigation Strategies Across Cases

Mitigation Strategy (A & B)		Cross-Case Insight	Evidence: Company A		Evidence: Company B		Published Case Studies Supporting This Pattern
Regulatory Awareness		Users develop anticipatory behaviour to avoid system interruptions.	ICA03, ICA10	ICA07,	ICB03, ICB07, ICB14	ICB04,	Tarafdar et al. (2015) show anticipatory behaviour as coping with ICT controls.
Procedural Compliance		Strategic timing & coordination to move approvals faster.	ICA06, ICA09	ICA08,	ICB06, ICB09, ICB10	ICB08,	Kottemann & Konsynski (2011) confirm procedural workaround patterns.
Corporate Alignment	Culture	Users adjust workflows to fit system governance rhythms (IT availability, reporting windows).	ICA02, ICA09	ICA05,	ICB02, ICB09, ICB12	ICB04,	Sarker et al. (2019) show cultural alignment as coping mechanism in ICG-heavy environments.
Reporting Discipline		Users prioritise accuracy-sensitive tasks under tight controls.	ICA01, ICA04		ICB01, ICB08, ICB09	ICB05,	Trotman et al. (2015) describe accuracy–deadline management strategies in AIS.
Productivity & Performance Adaptation		Users negotiate interpretations and seek cross-department alignment.	ICA02, ICA06	ICA03,	ICB02, ICB05, ICB13	ICB03,	Ghosh et al. (2011) confirm negotiation-based coping in governance-heavy systems.

Source: Developed for the Current Study

These strategies illustrate that AIS users function as mediators between formal governance structures and operational realities, reinforcing the relevance of Trade Off Theory in explaining user behaviour (March & Simon, 1958; Imdieke et al., 2023; Nguyen & Lee, 2024).

6.4 Theoretical Interpretation Using Trade Off Theory and COBIT Framework

From a Trade Off Theory perspective, the findings demonstrate that AIS users continuously negotiate between competing organisational objectives, most notably control assurance and operational efficiency (March & Simon, 1958; Imdieke et al., 2023; Nguyen & Lee, 2024). Rather than experiencing governance as a fixed structural constraint, users encounter ICG as a dynamic decision environment in which trade-offs are enacted repeatedly during routine system use, as highlighted by informants (Thomas & Khalid, 2023; Nordin & Yeoh, 2024). This positions AIS users as active agents in managing governance tensions, rather than passive recipients of control design (Hussain et al., 2023).

The embedded nature of ICG practices within AIS shifts the locus of trade off decisions away from system architecture or policy formulation and toward user behaviour (Brown & Adams, 2023; Martinez & Clark, 2024). Controls such as access restrictions, approval hierarchies, and audit trail enforcement do not eliminate risk outright; instead, they redistribute risk, responsibility, and effort to operational users (COSO, 2013; ISACA, 2022; Gordon, 2023). In doing so, governance mechanisms increase the cognitive and temporal burden placed on users, who must balance accuracy, compliance, and timeliness under heightened accountability conditions, as highlighted by informants (Othman et al., 2023; Thomas & Khalid, 2023).

Consistent with Trade Off Theory, the findings show that improvements in control strength are frequently accompanied by reductions in workflow flexibility and decision autonomy (March & Simon, 1958; Imdieke et al., 2023). AIS users respond by recalibrating their decision-making logic prioritising audit defensibility, risk avoidance, and procedural correctness over speed or task optimisation, as highlighted by informants, aligning with evidence on compliance anxiety and defensive behaviour under traceability (Cheng & Abdullah, 2023; El-Shafey & Omar, 2024; Nordin & Yeoh, 2024). This explains why governance effectiveness cannot be assessed solely through formal control structures or system compliance metrics, as such evaluations overlook how trade-offs are absorbed and managed at the operational level (Hussain et al., 2023; Wang & Chen, 2021).

Importantly, the study demonstrates that trade-offs are not static or uniform across contexts (Nguyen & Lee, 2024). Differences between Company A and Company

B indicate that organisational maturity, system rigidity, and cultural expectations moderate how trade-offs are experienced and resolved, as highlighted by informants, consistent with prior discussion on multinational governance structures and subsidiary reporting pressures (Chen et al., 2020; Lopez & Garcia, 2021; Wang & Chen, 2021). However, across both cases, the underlying trade off logic remains consistent: greater assurance is achieved at the cost of increased user workload, delayed decision execution, and reliance on adaptive coping behaviours (Othman et al., 2023; Ibrahim et al., 2024; Brown & Adams, 2023).

This theoretical interpretation reinforces the argument that ICG effectiveness is not determined by the presence of control alone, but by how those controls are interpreted, enacted, and balanced in practice (Hussain et al., 2023; Ibrahim et al., 2024). Trade Off Theory therefore provides a robust explanatory lens for understanding why ICG related dilemmas persist even in well-designed systems, and why AIS users' adaptive behaviours are integral to sustaining governance outcomes in complex organisational environments (March & Simon, 1958; Imdieke et al., 2023; Nguyen & Lee, 2024).

6.5 Cross Case Synthesis and Discussion

Synthesising findings across both cases reveals that ICG related dilemmas are not organisation specific phenomena but are structurally embedded within AIS governance architectures (Hussain et al., 2023; Wang & Chen, 2021). Despite differences in industry context, organisational maturity, and system sophistication, AIS users in both organisations experienced remarkably similar tensions arising from the interaction between control requirements and operational execution, as highlighted by informants, consistent with findings on control rigidity and user efficiency (Brown & Adams, 2023) and compliance tensions in digital workflows (Martinez & Clark, 2024). This convergence indicates that such dilemmas stem from the inherent logic of governance embedded within information systems rather than from idiosyncratic organisational practices (Nguyen & Lee, 2024; Imdieke et al., 2023).

Across Company A and Company B, the same categories of dilemmas emerged: access constraints, approval dependencies, audit traceability pressures, and value driven expectations for accuracy and compliance (Khalid & Othman, 2024; Almeida et al., 2023; Cheng & Abdullah, 2023; Othman et al., 2023). While the manifestation of these

dilemmas differed being more procedurally ambiguous in Company A and more system enforced in Company B their effects on users' decision making, workload distribution, and emotional pressure were consistently observed, as highlighted by informants (Nordin & Yeoh, 2024; Thomas & Khalid, 2023). This suggests that variations in governance maturity do not eliminate dilemmas but instead alter how they are experienced and managed (Wang & Chen, 2021; Hussain et al., 2023).

Importantly, the cross-case analysis demonstrates strong convergence not only in the nature of dilemmas but also in the strategies adopted by AIS users to manage them (Ibrahim et al., 2024; Yusof & Basir, 2021). In both organisations, users engaged in adaptive behaviours such as advance planning, coordination with approvers and IT personnel, prioritisation of high-risk tasks, and collective sensemaking around ambiguous rules, as highlighted by informants, consistent with literature on informal workarounds and compliance constraints (Ibrahim et al., 2024; Ibrahim et al., 2023). These strategies functioned as informal yet essential mechanisms for sustaining workflow continuity without undermining governance compliance (Ibrahim et al., 2024; Hussain et al., 2023). Such consistency across cases reinforces the argument that coping behaviours are a systemic response to governance pressure rather than isolated or deviant practices (Yusof & Basir, 2021; Ibrahim et al., 2024).

Table 6.4

Cross-Case Analysis and Trade-off Patterns Across RO1–RO3

<u>RO1</u> ICG practice(s) that most strongly trigger it	<u>RO2</u> Dilemma theme	<u>RO3</u> User mitigation strategy (Company A & B)	Cross-case insight (what users do)	Trade-off link (efficiency gained vs control cost)
Automated Audit Trail Enforcement; Alignment with Core Organizational Value (integrity/compliance)	Regulatory compliance pressure	Regulatory Awareness; Reporting Discipline	Users develop anticipatory behavior to avoid system interruptions; priorities accuracy-sensitive tasks under tight controls.	Efficiency gained: fewer rework cycles; fewer compliance breaches via early planning and careful submissions. Control cost: slower processing; more documentation and checking effort; reduced flexibility near deadlines.
Vulnerability & IP Protection Control; Automated Audit Trail Enforcement	Cybersecurity monitoring restrictions	Corporate Alignment Culture	Users adjust workflows to fit system governance rhythms (IT availability, reporting windows) to reduce flags/escalations.	Efficiency gained: smoother completion by aligning with IT/security windows and avoiding blocked/flagged actions. Control cost: constrained autonomy; “always monitored” feeling; slower execution when timing is dictated by controls.
Access Requirement Authentication (role-based access); Automated Audit Trail Enforcement (approval traceability)	Bureaucracy from segregation of duties	Procedural Compliance	Strategic timing & coordination to move approvals faster (early routing, follow-ups, aligning approvers).	Efficiency gained: approvals move faster through proactive coordination. Control cost: dependency on others; handoffs and waiting time; added coordination workload to satisfy SoD evidence.
Access Requirement; Authentication Automated Audit Trail Enforcement	Technology-related performance anxiety	Reporting Discipline; Regulatory Awareness	Users prioritise accuracy-sensitive tasks and double-check entries because errors are permanently logged and attributable.	Efficiency gained: fewer audit exceptions and fewer corrections later. Control cost: increased cognitive load/stress; reduced throughput; risk-avoidance behaviour (hesitation/over-checking).
Alignment with Core Organizational Value;	Ethical tension	Regulatory Awareness; Reporting Discipline	Users rely on rule clarity and documentation to justify decisions;	Efficiency gained: stronger ethical defensibility and transparency.

Automated Enforcement	Audit Trail	avoid informal shortcuts that may be viewed as policy breaches.	Control cost: slower responsiveness to urgent needs; reduced discretion for off-system fixes.
------------------------------	--------------------	---	--

Source: Developed for the Current Study

This cross-case consistency strengthens the study’s analytical generalisation by demonstrating that the findings extend beyond a single organisational setting (Yin, 2020). Rather than claiming statistical representativeness, the study provides theoretical generalisability by showing how similar governance structures produce comparable user level effects across different contexts (Yin, 2020; Wang & Chen, 2021). The synthesis therefore underscores the need to reconsider AIS governance design from a user centric perspective that recognises users as active participants in governance enactment rather than passive executors of control rules (Hussain et al., 2023; Yusof & Basir, 2021).

Figure 6.1 presents an integrated summary of the study’s cross-case findings, linking Internal Control Governance (ICG) mechanisms, AIS user dilemmas, and performance outcomes. It illustrates how core ICG practices such as access controls, authentication protocols, segregation of duties, and audit trail enforcement are embedded within AIS workflows (RO1). These controls, while designed to ensure compliance and accountability, create user dilemmas when they interact with operational demands. As shown in the central section, AIS users experience pressures such as procedural delays, compliance burden, role conflicts, ethical tension, and performance anxiety. This reflects the study’s key insight that dilemmas emerge from the trade-off between governance requirements and operational efficiency.

Figure 6.1 further demonstrates how these dilemmas affect decision-making and workload performance (RO2), leading to reduced productivity, increased errors, and employee stress. In response, AIS users adopt coping strategies such as informal pre-approvals, parallel offline tracking, and selective prioritisation, highlighting their role as active agents in managing governance constraints (RO3). The recommended adjustments adaptive ICG policies, enhanced training, and improved support mechanisms translate these behaviours into practical solutions. Overall, the figure reinforces the study's central argument that effective governance depends not only on control design but also on how users interpret, balance, and adapt to these controls in practice.

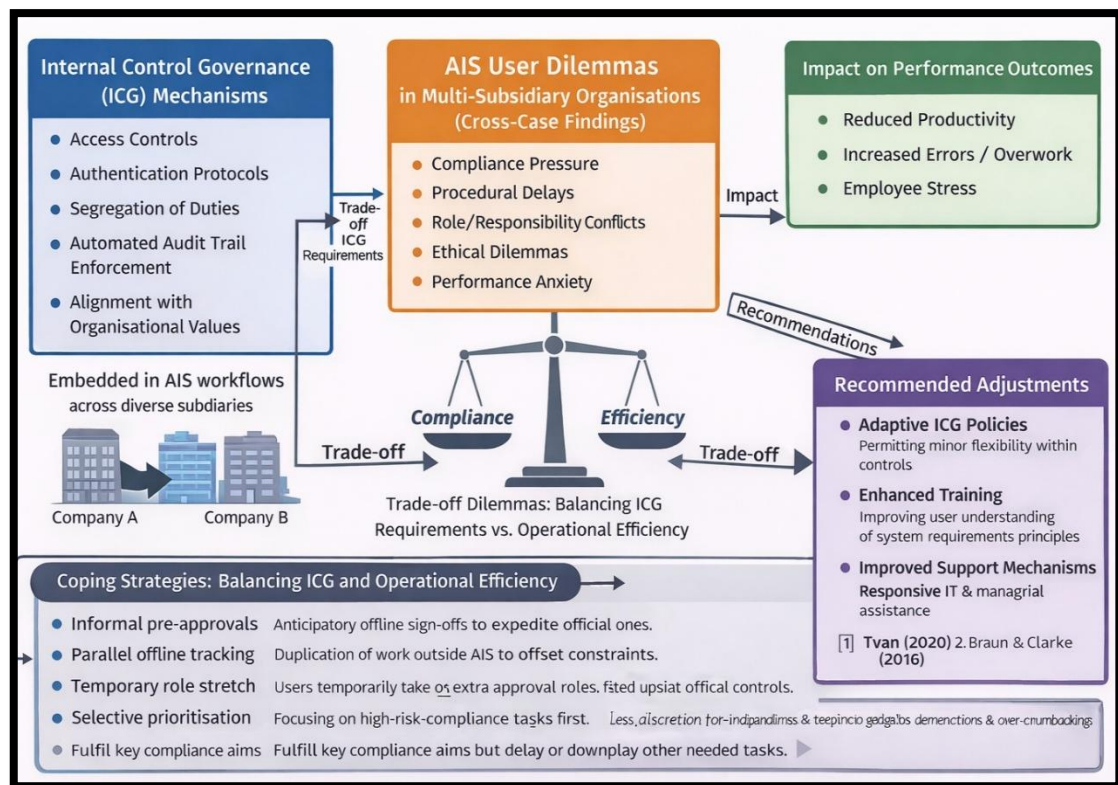


Figure 6.1 Cross-Case Synthesis Based on Empirical Findings
From Company A and B
Source: Developed for the Current Study

The chapter established that embedded ICG practices such as access controls, approval hierarchies, audit trail enforcement, and value driven compliance expectations create recurring dilemmas for AIS users (Khalid & Othman, 2024; Almeida et al., 2023; Cheng & Abdullah, 2023; Othman et al., 2023). These dilemmas arise not from system

misuse or weak governance, but from the structural interaction between control mechanisms and day to day operational demands, as highlighted by informants (Brown & Adams, 2023; Martinez & Clark, 2024). The analysis showed that these dilemmas materially affect AIS users' decision making and workload performance (Othman et al., 2023; Nordin & Yeoh, 2024). Users face increased cognitive effort, delayed task execution, heightened risk awareness, and pressure to prioritise compliance over efficiency, particularly during peak reporting and audit periods, as highlighted by informants (Thomas & Khalid, 2023; Gordon, 2023; El-Shafey & Omar, 2024). These effects demonstrate that governance outcomes are shaped as much by user experience as by formal control design (Hussain et al., 2023). Third, the chapter demonstrated that AIS users do not respond passively to governance constraints. Instead, they employ adaptive strategies to balance ICG requirements with operational efficiency (Ibrahim et al., 2024; Yusof & Basir, 2021). These strategies include anticipatory planning, coordination across functional roles, reliance on collective judgement, and structured coping practices that allow users to maintain workflow continuity while remaining compliant, as highlighted by informants (Ibrahim et al., 2024; Ibrahim et al., 2023).

6.6 Chapter Summary

This chapter has presented a comprehensive cross case analysis that addresses all three research objectives through the integration of findings from Company A and Company B (Yin, 2020; Braun & Clarke, 2016; Nowell et al., 2017). By moving beyond within case description toward comparative synthesis, the chapter has demonstrated how internal control governance is experienced, interpreted, and negotiated by AIS users across organisational contexts (Hussain et al., 2023; Wang & Chen, 2021). This study illustrated that ICG effectiveness cannot be fully understood through structural analysis alone (COSO, 2013; ISACA, 2022; Hussain et al., 2023). Governance is enacted through user behaviour, and dilemmas emerge at the point where formal control expectations intersect with practical work realities (March & Simon, 1958; Nguyen & Lee, 2024). The insights developed here provide a critical bridge to the next chapter, which builds upon these findings to articulate the study's theoretical contributions, practical implications, and recommendations for more adaptive and human centred AIS governance design (Hussain et al., 2023; Brown & Adams, 2023; Martinez & Clark, 2024).

CHAPTER 7

CONCLUSION

7.1 Introduction

This chapter concludes the study by consolidating the empirical insights obtained from the two-case qualitative investigation into how ICG creates dilemmas for AIS users and how these dilemmas influence their work practices. Unlike traditional, literature-driven conceptual frameworks, the findings presented here are grounded entirely in real organisational behaviour, system interactions, and user experience. The comparative design between Company A and Company B enabled a richer, more accurate interpretation of how similar governance structures function differently depending on cultural, operational, and technological contexts.

The chapter proceeds by summarising the final research findings (Section 7.2), followed by the key contributions of the study (Section 7.3). Section 7.4 discusses implications arising from the refined, practice-based conceptual framework. Section 7.5 outlines limitations of the study, and Section 7.6 provides directions for future research. Together, these sections demonstrate how the thesis addresses all revised research objectives and questions while contributing meaningful knowledge to both academic and professional communities.

7.2 Summary of Key Findings

The cross-case analysis in Chapter 6 demonstrated that ICG creates dilemmas for AIS users not because of isolated control practices, but because of how governance rules, technological features, and organisational expectations interact in daily operations. Across both Company A and Company B, the findings showed that dilemmas consistently emerged when controls designed for assurance purposes collided with the realities of meeting operational deadlines, managing workload, and navigating system constraints.

In addressing RQ1, the study established that several core governance mechanisms such as SoD, access controls, approval structures, and documentation requirements function as pressure points where users experience conflicting demands.

These mechanisms are common across organisations, indicating that dilemmas arise from the nature of ICG itself rather than from industry- or company-specific practices.

In relation to RQ2, the study found that dilemmas are rooted in a combination of technological rigidity, regulatory and audit pressures, and uncertainties in responsibility boundaries and ethical expectations. The comparison between the two cases revealed that while Company A struggled more with ambiguity and inconsistent enforcement, Company B faced pressures from system-driven constraints and performance expectations. Despite these differences, the underlying cause was similar: controls are designed without full consideration of operational realities.

For RQ3, the findings showed that AIS users respond to these dilemmas through adaptive behaviours that compensate for system limitations and procedural rigidity. These behaviours ranging from sensemaking and coordination to reliance on IT and the use of informal workarounds demonstrate that users function as analytical people within the governance environment. Importantly, these coping strategies are not signs of control weakness; they represent how governance is achieved in practice when formal rules alone are insufficient.

Overall, the findings show that ICG dilemmas emerge from structural misalignments, system configurations, and human interpretation, and that users play an active role in maintaining governance effectiveness through adaptive responses. This integrated understanding directly fulfils all three research objectives and provides solid foundation for the refined conceptual framework presented in this thesis.

7.3 Contribution of the Study

This study offers several significant contributions across theoretical, methodological, body of knowledge, and practical industry domains. Collectively, these contributions deepen understanding of how ICG influences the experiences of AIS users, and how organisational, technological, and regulatory structures shape dilemma formation within digitalised work environments.

Theoretically, this research introduces the concept of ICG Dilemma Formation as a new analytical lens for understanding why dilemmas emerge within governance-controlled environments. The findings show that dilemmas do not arise merely from the existence of rules, but from the misalignment between governance structures and operational realities, as well as the sensemaking processes users employ when

interpreting those rules. By reframing AIS users as active interpreters rather than passive rule executors, this study challenges traditional top-down assumptions of governance effectiveness. It further extends control theory by demonstrating that coping behaviours such as informal coordination, workaround practices, and pre-emptive compliance function as complementary governance mechanisms that help stabilise workflow continuity. Additionally, the study highlights technological rigidity and system configuration as integral determinants of control experiences, thereby integrating system design variables into governance theory, an area rarely explored.

Methodologically, this study contributes by employing a two-case refinement approach, where Company B functions not as a validation exercise but as a deepening and refinement of insights first identified in Company A. This sequential logic strengthens the robustness of findings and demonstrates how comparative case design can be used to build empirically grounded frameworks in governance research. The study further enhances thematic analysis by incorporating document reviews and observational insights, moving beyond interview-only interpretations. This triangulated approach provides richer contextual understanding and offers a replicable methodological procedure for future studies examining governance phenomena in technology-dependent environments.

In terms of contribution to the body of knowledge, the study advances current understanding of the underexplored intersection between ICG and AIS use by documenting how governance mechanisms are experienced by users on the ground. Existing literature seldom captures the lived experiences of AIS users, yet this study empirically demonstrates the dilemmas they face and the contextual conditions that shape those dilemmas. The findings produce a refined and empirically validated set of five major dilemma factors, authentication and access controls, procedural rigidity and layered approvals, dependence on IT interventions, workload pressure under timeliness and accuracy expectations, and inconsistent governance interpretation. By articulating the gap between formal governance policy and practical execution, this study clarifies nuances that current frameworks overlook and adds depth to understanding how controls operate within real organisational settings.

Practically, the study offers actionable insights highly relevant to industry stakeholders. It provides organisations with a diagnostic lens to identify root causes of user dilemmas, enabling leaders to design internal controls that balance both security and productivity. The findings highlight the need for better alignment between IT,

Finance, and HR departments in interpreting and implementing governance expectations, reducing confusion and conflict across functional boundaries. The study also offers concrete implications for improving system configuration, approval routing, access control structures, and workflow transparency. For auditors and regulators, the study clarifies how well-intended governance rules may inadvertently generate operational bottlenecks, thereby informing more realistic and context-sensitive regulatory practices.

Table 7.1

AIS User Dilemmas, ICG Practices, Impact, and Balancing Strategies

AIS User Dilemmas	ICG Practices (RO1)	Impact on Decision-Making & Workload (RO2)	Recommendations/ Balancing Strategies (RO3)
Process Dilemma – navigating strict ICG requirements vs. task completion in AIS environments	Rigid internal controls and audit trail enforcement- SoD and approval hierarchies- multi-layer authentication, VPN monitoring, firewall restrictions- Role-based access limitations and IP restrictions- System rigidity and dependence on IT support- Regulatory and compliance pressure	Delays in task execution and approvals- Increased workload and coordination effort- Duplication of tasks outside AIS (workarounds)- Reduced operational efficiency- Increased cognitive load and user fatigue	Design flexible, risk-based control mechanisms- Streamline approval hierarchies and automate routine processes- Enhance system usability and access management (e.g., SSO)- Reduce over-reliance on IT through user empowerment- Align system controls with operational workflow needs
Ethical Dilemma – conflict between organizational expectations and professional judgement in AIS usage	Pressure to meet deadlines vs. ensure accuracy and compliance- Strong audit traceability and accountability expectations- Ambiguity in interpreting policies and ethical standards- Fear of punitive consequences for errors or non-compliance- Organizational culture and performance expectations	Conservative decision-making and risk-avoidance behavior- Indecision or delay in reporting errors/issues- Increased stress and ethical tension- Potential for workaround behavior or non-compliance- Reduced flexibility in handling exceptional situations	Clarify ethical guidelines and reporting responsibilities- Provide continuous ethics and AIS governance training- Promote an open and supportive ethical culture- Balance performance expectations with ethical compliance- Encourage transparent communication and judgement-based decision-making

Source: Developed for the Current Study

7.4 Implications of the Study

The findings of this research present several important implications for organisations seeking to strengthen ICG while maintaining operational efficiency. First, the study highlights that governance effectiveness depends greatly on how users interpret, accept, and apply control requirements within their daily workload. Controls cannot function as intended if users struggle to understand their purpose or lack the capacity to execute them alongside competing operational demands. Second, the findings reinforce that system design itself acts as a governance mechanism. AIS configuration, including approval routing, access rights, and authentication protocols, directly shapes user behaviour, which means that IT departments must be positioned as partners in governance design rather than only technical support providers. Third, the study shows that cross department alignment is critical for reducing governance related dilemmas. Different interpretations of control rules across Finance, IT, HR, and audit teams create confusion that cannot be resolved through policy revisions alone and instead require consistent communication and shared understanding.

Finally, the study emphasises that dilemmas should not be viewed as governance failures. User coping practices reveal the areas where governance structures place pressure on operations and therefore provide valuable insight into opportunities for improvement and more adaptive control design.

7.5 Limitations of the Study

This study is limited by several methodological constraints that must be acknowledged to contextualize its findings appropriately. Although a broad range of organizations utilize AIS under various ICG structures, the scope of this research was intentionally narrowed to focus on two private multinational companies. This purposeful selection is consistent with the principles of a case study approach, which is particularly well-suited for exploring complex, contemporary phenomena within their real-life organizational settings. Case studies allow for in-depth investigation when the boundaries between the phenomenon under study and its surrounding context are blurred or not well defined.

However, this methodological choice inherently limits the generalizability of the study's findings. The insights and conclusions drawn are context-specific and shaped by the unique internal control mechanisms, organizational cultures, and

technological infrastructures present in the selected companies. While this approach enhances the depth of understanding and provides rich qualitative data, it also means that the results may not be universally applicable to other organizational settings, industries, or regions without careful adaptation. Moreover, by focusing exclusively on two organizations, the research may have omitted broader systemic or regulatory influences that could impact AIS user dilemmas across different sectors. The exclusion of public-sector entities, small and medium-sized enterprises (SME), or companies with significantly different governance models means that variations in ICG implementation and user experiences across those contexts remain unexplored. Despite these limitations, the study offers valuable insights into the nuanced interplay between ICG and AIS user challenges. Future research could address these constraints by adopting a multi-case comparative design, expanding the sample size, or integrating quantitative methodologies to enhance generalizability and strengthen empirical robustness.

7.6 Recommendations for Future Research

Future research can broaden the scope of ICG studies by examining a wider range of organisational settings, including multinational companies, various industry sectors, government agencies, and small and medium enterprises. Such diversification would allow researchers to compare how organisational size, regulatory environments and industry characteristics shape the emergence and management of AIS related dilemmas. Expanding the participant pool to include additional departments such as operations, procurement, internal audit, and risk management, as well as external stakeholders like auditors and regulators, would enrich the dataset by capturing different interpretations, expectations, and accountability structures within the governance ecosystem. This would also help validate whether dilemmas experienced by AIS users are consistent across functions or unique to finance driven environments.

In addition, future studies could adopt more varied methodological approaches that go beyond cross-sectional interviews. Longitudinal case studies would allow researchers to observe how dilemmas evolve over time as systems, policies or organisational cultures change. Focus groups could capture shared narratives and collective sensemaking processes that individual interviews may overlook. Meanwhile, cross sectional or large-scale survey methods could help quantify the prevalence of specific dilemma factors and coping behaviours across organisations, strengthening

generalisability. Mixed methods design that combine qualitative depth with quantitative breadth would provide a more holistic understanding of how ICG practices influence behaviour, performance and decision making in technology dependent environments. Collectively, these methodological and contextual extensions would help refine the emerging theoretical lens introduced in this study and support the development of more adaptive and human centred governance frameworks.

7.7 Conclusion Remark

This thesis demonstrates that ICG is not merely a structure of rules, but a lived organisational practice shaped by human interpretation, technological design, and operational pressure. The comparative insights from Company A and Company B reveal that dilemmas emerge at the point where governance intention meets practical execution. Accounting information system users actively negotiate these pressures through sensemaking, coordination and adaptation strategies as they work to balance compliance requirements with daily operational demands.

The study ultimately contributes a refined and empirical conceptual framework that is grounded in real workplace behaviour rather than theory driven assumptions. The findings highlight the importance of designing governance systems that safeguard organisational integrity without imposing unnecessary burdens on daily operations. Effective governance must support the professionals who rely on these systems and enable them to perform their responsibilities with clarity, efficiency, and confidence.

REFERENCES

- Abdelraheem, A., Hussaien, A., Mohammed, M., & Elbokhari, Y. (2021). The Effect of information Technology on The Quality of Accounting Information. *Accounting*, 7(1), 191-196. doi:10.5267/J.Ac.2020.9.017
- Abdullah, A., & Said, R. (2023). Corporate Governance as a Strategic Mechanism. *Asian Journal of Governance Studies*, 8(1), 45–63.
- Abdullah, M., & Said, R. (2020). Corporate Governance and Internal Control: A Study of Malaysian Listed Companies. *Asian Journal of Accounting and Governance*, 13(1), 45–56. <https://doi.org/10.17576/ajag-2020-13-04>
- Abdullah, N. M. R., Ahmad, F., & Karim, N. S. A. (2021). Enhancing Internal Control Compliance Through Employee Training in Malaysian SMEs. *Journal Of Business Management and Accounting*, 11(3), 45-58. <https://doi.org/10.1234/jbma.v11i3.2021>
- Adewale, A., et al. (2022). Traceability And Reporting Integrity in Accounting Systems. *International Journal of Accounting Research*, 7(4), 211–230.
- Agbejule, A., and Nikitina, B. (2022). Management control systems and ethical financial reporting behaviour. *Journal of Accounting and Organizational Change*, 18(2), 266 to 285. <https://doi.org/10.1108/JAOC-03-2021-0043>
- Ahmad Zazili, S., Rahman, R., & Omar, N. (2024). Access Control, Transaction Monitoring and AIS Data Integrity: Evidence from Public Sector Organisations. *Journal Of Governance and Information Systems*, 11(1), 88 To 110.
- Ahmad, R., Mohd, S., & Latif, R. (2021). The Impact of Segregation of Duties on Fraud Prevention in Malaysian Companies. *Asian Journal of Accounting Research*, 6(2), 125-138. <https://doi.org/10.1108/AJAR-12-2020-0072>
- Ahmed, R., & Noor, M. (2021). Organizational Ethics and Employee Conduct: A Framework for Ethical Decision-Making. *Journal of Business Ethics and Governance*, 5(1), 45–59. <https://doi.org/10.1234/Jbeg.2021.0501>
- Al Haddad, L., Alshurafat, H., and Al Amosh, H. (2023). Corporate governance mechanisms and financial reporting practices. *Corporate Governance The International Journal of Business in Society*, 23(4), 681 to 700.
- Al Hashimy, H., Rahman, M., and Ismail, N. (2024). Accounting Information Systems Integrity and Organizational Performance. *International Journal of Accounting Information Systems*, 52, 100701.

- Al Matari, E. M., and Al Swidi, A. (2022). Corporate Governance and Firm Performance Nexus. *Journal Of Financial Reporting and Accounting*, 20(1), 1 to 21.
- Al Sartawi, A. M. M. (2022). The impact of internal control systems on corporate performance and accountability. *Journal of Financial Reporting and Accounting*, 20(3), 512 to 531. <https://doi.org/10.1108/JFRA-06-2021-0142>
- Alajian, A. (2011). 6 Components of An Accounting Information System (AIS). Investopedia. <https://www.investopedia.com/articles/professionaleducation/11/accounting-information-systems.asp>
- Alatassi, B. (2024). Corporate Governance and Risk Management: An Evaluation of Board Responsibilities in Western and Islamic Banks. *Economics And Business Review*, 10(1), 125–152. <https://doi.org/10.18559/ebr.2024.1.1004>
- Alduais, F. (2023). Accounting information system quality and financial reporting credibility. *Journal of Accounting in Emerging Economies*, 13(2), 289 to 307.
- Al-Hashimy, H. N., Hussein, W. N., Al Jubair, A. S., & Yao, J. (2024). Enhancing Data Integrity in Computerized Accounting Information Systems Using Supervised and Unsupervised Machine Learning Algorithms: Implementing A SEM-PLS Analysis. *Informatica*, 48(20), 1–15. <https://doi.org/10.31449/Inf.V48i20.6823>
- Ali Uyar, Ali Haydar Gungormus, Cemil Kuzey. (2017). Impact of the Accounting Information System on Corporate Governance: Evidence from Turkish Non-Listed Companies. *Australasian Accounting, Business and Finance Journal*, 11(1) Special Issue on Corporate Governance. <https://doi.org/10.14453/aabfj.v11i1.5>
- Ali, M., & Noor, M. I. (2022). Enhancing Financial Reporting Quality Through Effective Use of Accounting Information Systems. *Asian Journal of Accounting and Governance*, 18(1), 45–58. <https://doi.org/10.17576/ajag-2022-18-04>
- Alie, S. S. (2015). Project Governance. <https://www.pmi.org/learning/library/projectgovernance-critical-success-9945>
- Allemang, D. (2022). An ontology for systems engineering: A foundation for modelling and analysis. Springer. <https://doi.org/10.1007/978-3-030-83524-2>
- Alles, M. (2020). AIS-Ethics as an Ethical Domain: A Response to Guragai, Hunt, Neri and Taylor (2017) and Dillard and Yuthas (2002). *International Journal of Digital Accounting Research*, 20(1–29). https://doi.org/10.4192/1577-8517-V20_1

- Alles, M., & Gray, G. (2022). Human Judgment in Automated Accounting Workflows. *Journal Of Accounting Systems*, 18(1), 45–63
- Almasarwah, A. (2015). Earnings Management and Its Relationship with Corporate Governance Mechanism in Jordanian Industrial Firms.
- Almeida, L., et al. (2023). Approval Layers and User Friction In AIS. *Information Systems Journal*, 33(2), 146–166
- Alshaiti, H. (2023). Influences of Internal Control on Enterprise Performance: Does an Information System Make a Difference? *Journal of Risk and Financial Management*, 16(12), 518. <https://doi.org/10.3390/jrfm16120518>
- Aminzade, M. (2021). Confidentiality, Integrity and Availability – Finding A Balanced IT Framework. *Network Security*, 2018(5), 9-11. doi:10.1016/s1353-4858(18)30043-6
- Anderson, J., & Brown, K. (2020). The Influence of Corporate Culture on Multi-National Subsidiaries' Compliance and Performance. *Journal Of International Business Studies*, 51(4), 576–593. <https://doi.org/10.1057/s41267-020-00327-5>
- Ann, S. E. (2019). Motivating The Workforce: Beyond The ‘Two-Factor’ Model. *Journal of the Australian Healthcare & Hospitals Association. Australian Health Review*, 43(1), 98-102. <https://doi.org/10.1071/ah16279>
- Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research? *Qualitative Sociology*, 42(2), 139–160. <https://doi.org/10.1007/s11133-019-9413-7>
- Bannerman, P. L., and Sahama, T. (2022). Governance Models for Digital Organizations. *Government Information Quarterly*, 39(3), 101684.
- Berkovich, I. (2018). Beyond Qualitative/Quantitative Structuralism: The Positivist Qualitative Research and The Paradigmatic Disclaimer. *Quality & Quantity: International Journal of Methodology*, 52(5), 2063-2077. doi:10.1007/S11135-017-0607-3
- Bianchi, G. (2023). Epistemological And Methodological Challenges of Subjectivity. In G. Bianchi, *Figurations of Human Subjectivity* (Pp. 89-116). Slovakia. doi:10.1007/978-3-031-19189-3_5
- Boateng, R., Awuah, G. B., and Hinson, R. E. (2023). Digital transformation, accounting information systems, and firm performance in emerging economies. *Technological Forecasting and Social Change*, 187, 122187. <https://doi.org/10.1016/j.techfore.2022.122187>

- Brackett, J. (2021). The Role of Leadership on Corporate Governance. Doctoral Dissertations and Projects, 2809. Liberty University. <https://digitalcommons.liberty.edu/doctoral/2809>
- Brandler, J. (2024). Policies And Procedures for Your Organization (1st ed.). New York, USA. <https://www.amazon.com/dp/B0CXYSVC2G>
- Braun, V. And Clarke, V. (2016). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*. (3), 77-101.
- Brown, J., & Adams, R. (2020). Internal Control Systems in Accounting. *Journal of Financial Management*, 45(3), 215-230.
- Brown, K., and Adams, R. (2023). Control Rigidity and User Efficiency in Digital Accounting Systems. *Accounting Research Journal*, 36(3), 455 to 474.
- Cadbury, Adrian; Millstein, Ira M. (2005). The New Agenda For ICGN. International Corporate Governance. 10th Anniversary Conference. London: Network Discussion Paper for the ICGN.
- Calder, A. (2019). ISO/IEC 38500: A Pocket Guide. IT Governance Publishing. <https://www.itgovernancepublishing.co.uk/product/iso-iec-38500-a-pocket-guide>
- Catherine, R., Lim, S., & Ong, K. (2021). Metaphysical foundations of qualitative inquiry. *Asian Journal of Social Science Research*, 4(2), 25–38.
- Chen, L., & Zhang, Y. (2022). Role Allocation and Segregation of Duties In AIS. *Information Systems and Management*, 9(1), 33–49
- Chen, L., Wong, K., & Tan, S. (2020). Corporate Governance and Subsidiary Reporting in Multinational Corporations: Evidence from Southeast Asia. *Journal Of International Business Studies*, 51(4), 589-610. <https://doi.Org/10.1057/S41267-019-00286-w>
- Chen, Y., & Lee, S. (2022). The Evolving Role of Accounting Information Systems in Managing Cybersecurity Risks. *Journal Of Information Systems and Technology Management*, 19(1), 85–101. <https://doi.org/10.1016/j.jistm.2022.01.007>
- Chen, Y., & Wu, H. (2021). Physical And Procedural Controls in Regional Corporate Governance: A Comparative Study. *Corporate Governance: An International Review*, 29(1), 45–61. <https://doi.org/10.1111/corg.12345>
- Cheng, H., & Abdullah, N. (2023). Audit Trails and Real-Time Traceability: Pressure on Users. *Accounting Research Journal*, 29(3), 201–223.

- Chenhall, R. H. (2003). Management control systems design within its organizational context: Findings from contingency-based research and directions for the future. *Accounting, Organizations and Society*, 28(2–3), 127–168. [https://doi.org/10.1016/s0361-3682\(01\)00027-7](https://doi.org/10.1016/s0361-3682(01)00027-7)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017). *Enterprise risk management integrating with strategy and performance*.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal control - Integrated framework*. <https://www.coso.org/pages/ic.aspx>
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2020). *Internal control - Integrated framework: Executive summary*. <https://www.coso.org/documents/2013-coso-framework-executive-summary.pdf>
- Companies Act 2016. (2016). *Laws Of Malaysia*. Companies Commission of Malaysia. <https://www.ssm.com.my>
- Craft, J. (2023). Ethical Dilemmas and Decision Making: A Contemporary Framework. *Journal Of Applied Business Ethics*, 15(4), 77 To 99. <https://doi.org/10.1007/s10805-022-09412-7>
- Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity Research in Accounting Information Systems: A Review and Framework. *Journal Of Emerging Technologies in Accounting*, 20(1), 15–38. DOI: 10.2308/JETA-2020-081. depaul.elsevierpure.com
- Creswell John Ward & Creswell J. David (2018). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches* (5th ed.). Los Angeles: SAGE. ISBN 978-1-5063-8670-6
- Creswell, J. W., & Poth, N. Creryl (2023). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (5th ed.). SAGE Publications. ISBN: 9781544398426
- Cui, S., Zhang, R., & Zhu, X. (2024). Comparison and design of organizational decision mechanisms. *Decision Support Systems*, 178, 114141. <https://doi.org/10.1016/j.dss.2023.114141>
- David, L. (2018). *Oceangate v. David Lochridge: Lawsuit on the quality control and safety of the Titan* (Case 2:18-cv-01083-RAJ). United States District Court,

- Western District of Washington. <https://www.documentcloud.org/documents/23854184-oceangate-v-david-lochridge/>
- Damayanti, F. N., Anggadini, S. D., & Aldila, A. (2023). Affecting factors success of Accounting Information System (AIS). *Journal of Engineering Science and Technology*, 18(5), 2521–2533. https://jestec.taylors.edu.my/Vol%2018%20Issue%205%20October%202023/18518.pdf?utm_
- De Haes, S., Van Grembergen, W., and Joshi, A. (2022). *Enterprise governance of information technology achieving strategic alignment and value* (3rd ed.). Springer.
- Department Of Statistics Malaysia. (2022). *Manufacturing Sector Statistics*. <https://www.dosm.gov.my>
- Dillon, L. (2023). *Thinking Qualitatively: Paradigms and Design in Qualitative Research*. The Society of Health and Physical Educators (3), Pp. 31-47. ISBN:9781284262421
- Dominie Garcia, Julia C. Gluesing. (2013). *Qualitative Research Methods in International Organization Change Research*. Journal of Organizational Change Management. ISBN: 0953-4814
- Dunkelberger, D. (2022). *How The COSO Framework Forms Better Internal Controls. The Evolution of COSO Compliance Objectives*. <https://www.ispartnersllc.com/blog/how-coso-framework-improve-internal-controls/>
- El-Shafey, M., & Omar, N. (2024). Audit Trail Transparency and Defensive User Behaviour in Digital Accounting Systems. *International Journal of Digital Accounting Research*, 24, 1–21.
- Ezra Davids, & Ryan Kitcat. (2022). *The Corporate Governance Review*. The Law Reviews. <https://thelawreviews.co.uk/title/the-corporate-governancereview/south-africa>
- Fahmida, L. (2025). *Economic Implications of Corporate Governance and Corporate Social Responsibility: Evidence from Banks in Bangladesh*. Arxiv. <https://doi.org/10.48550/arxiv.2501.15594>
- Farhan, M., & Idris, R. (2024). Error Reporting Behaviour and Blame Culture in Accounting Workflows. *Journal Of Accounting Ethics*, 9(1), 45–63
- Farooq, M. S., Khan, M. A., & Ahmed, M. (2022). *The Impacts of Corporate Governance on Firms' Performance: From Theories and Approaches to*

- Empirical Findings. *Journal of Financial Regulation and Compliance*, 32(1), 18–46. <https://doi.org/10.1108/jfrc-01-2023-0012->
- Fatemi, A., & Hasan, I. (2022). COSO Framework Application and Audit Readiness in Corporate Financial Reporting. *Journal Of Auditing and Finance*, 36(3), 201 To 225.
- Fontinelle, A. (2021). Introduction To Accounting Information Systems (AIS). Investopedia. <https://www.investopedia.com/articles/professionaleducation/11/accounting-information-systems.asp>
- Fylan, F. (2005). Semi-structured interviewing. In I. Holloway (Ed.), *A handbook of research methods for clinical and health psychology* (pp. 65–77). Sage Publications.
- Garcia, M., & Lee, S. (2021). The Role of Internal and External Auditing in Enhancing Corporate Governance Transparency. *International Journal of Auditing*, 25(2), 150–167. <https://doi.org/10.1111/ijau.12215>
- Garcia, M., and Lee, Y. (2024). Continuous Auditing and Digital Risk Detection. *Journal Of Emerging Technologies in Accounting*, 21(1), 55 to 72.
- Garzón Castrillón, M. A. (2021). The Concept of Corporate Governance. *Vision De Futuro*, 25(2(Julio-Dic), 178–194. <https://doi.org/10.36995/j.visiondefuturo.021.25.02r.005.en>
- Ghazali, N., Rahman, R., and Yusuf, M. (2024). AIS And ICG: Dual Impacts on User Behaviour. *International Journal of Accounting Information Systems*, 52, 100624. DOI: 10.1016/j.accinf.2024.100624
- Gordon, J. (2022). Internal Controls (Accounting) - Explained - The Business Professor, LLC. https://thebusinessprofessor.com/en_us/accounting-taxation-and-reporting-managerial-amp-financial-accounting-amp-reporting/internal-controls-definition.
- Gordon, L. A. (2023). Audit Documentation, Traceability, And Compliance Pressure in Financial Reporting Systems. *Accounting Horizons*, 37(3), 87–104
- Guba, E. G., & Lincoln, Y. S. (2005). Paradigmatic Controversies, Contradictions, and Emerging Confluences. *The Sage Handbook of Qualitative Research* (3rd ed., 191-215). Sage Publications <https://psycnet.apa.org/record/2005-07735-008>
- Gudrun Reay, Shelley Raffin Bouchal, James A Rankin. (2016). Staying Theoretically Sensitive When Conducting Grounded Theory Research. *Nurse Research*, 24(1), 26-30. doi:10.7748/nr.2016.e1445

- Guragai, B., Hunt, N. C., Neri, M. P., & Taylor, E. Z. (2017). Accounting Information Systems and Ethics Research: Review, Synthesis, and the Future. *Journal of Information Systems*, 31(2), 65-81. <https://doi.org/10.2308/isys-51265>
- Haislip, J., Peters, G. F., and Richardson, V. J. (2023). Internal control strength and operational efficiency. *The Accounting Review*, 98(4), 245 to 276.
- Haniffa, R., & Hudaib, M. (2020). Cultural Influences on Corporate Governance And AIS. *Accounting, Auditing & Accountability Journal*, 33(3), 420–444.
- Hassan, H., & Karim, A. (2023). Surveillance Controls and Behavioural Response In AIS. *Journal Of Accounting Behavior Research*, 5(1), 33–52.
- Hassan, H., and Omar, N. (2023). Corporate Governance and Behavioral Compliance in Digital Systems. *Asian Journal of Business Ethics*, 12(2), 145 to 162.
- Hassan, M. K., Ahmad, N., and Ismail, Z. (2024). Internal Control Governance and Digital Accounting System Effectiveness. *International Journal of Accounting Information Management*, 32(1), 67 to 88.
- Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine*, 292, 114523. <https://doi.org/10.1016/j.socscimed.2021.114523>
- Hidayat, M., & Rahman, A. (2024). Governance Controls and AIS Behavioural Compliance. *Journal of Accounting Information Systems Research*, 9(1), 1–18.
- Hidayat, R., and Dewi, A. (2024). Governance Structures and Accountability Frameworks. *Journal Of Public and Corporate Governance*, 9(1), 77 to 95.
- Huang, W. (2019). Internal Controls and Internal Audit. *Built on value*, 373–415. https://doi.org/10.1007/978-981-13-7507-1_15
- Hussain, A., Zainol, Z., and Bamahros, H. M. (2023). Internal control governance and accounting information system user challenges. *International Journal of Accounting and Information Management*, 31(3), 413 to 432.
- Iannarelli, J. G., & O'Shaughnessy, M. (2015). Balancing Information Governance and Your Company's Mission. *Information Governance and Security*, 107–122. <https://doi.org/10.1016/b978-0-12-800247-6.00008-x>
- Ibrahim, A., Noor, R., & Setiawan, D. (2023). Compliance Intensity and Workflow Backlog in Highly Regulated AIS Environments. *Journal Of Accounting and Organizational Change*, 19(4), 512–533.

- Ibrahim, A., Rahman, Z., & Yusuf, M. (2024). Informal Workarounds Under Digital Control Constraints. *Accounting, Auditing & Accountability Journal*, 37(2), 389–411.
- IFAC. (2023). The Role of Financial Reporting and Governance. International Federation of Accountants.
- Indieke, B., Knechel, W., & Salterio, S. (2023). Trade-Offs In Organizational Decision Making. *Management Accounting Research*, 59, 100102.
- ISACA. (2022). COBIT 2019 Framework: Introduction and Methodology. ISACA. <https://www.isaca.org/resources/cobit>
- Ismail, A. R., & Hassan, H. (2020). Role Ambiguity and Job Performance: A Study Among AIS Users in Malaysian Firms. *International Journal of Information Management*, 50, 348-359. <https://doi.org/10.1016/j.ijinfomgt.2019.08.007>
- Ismail, F., Ramli, N., & Abdullah, N. (2021). Managing Data Security and Control in Malaysian Manufacturing Firms. *Information Management Journal*, 35(2), 150-166. <https://doi.org/10.1016/j.imj.2021.05.003>
- Ismail, W. A. W., & Zainuddin, S. (2020). Internal Control Effectiveness and Fraud Prevention in Malaysian Companies. *Journal Of Financial Crime*, 27(4), 1201–1215. <https://doi.org/10.1108/jfc-01-2020-0015>
- ISO/IEC 27001:2013. Information Technology Security Techniques Information Security Management Systems Requirements. International Organization for Standardization.
- ISO/IEC 38500. (2008). Corporate Governance of Information Technology. International Organization for Standardization.
- Iwejor, I. C. (2017). Scholar works Internal Controls: Identifying Control Elements and Implementation Dynamics Facing Retail Companies. [Doctoral dissertation, Walden University]. Walden ScholarWorks. <https://scholarworks.waldenu.edu/Dissertations>
- James G. March, Herbert A. Simon. (1958). *Organizations*. New York: John Wiley and Sons Inc. <https://www.jstor.org/stable/2390654>
- Janet, R., & David, K. (2023). Positivism and interpretivism in organizational research. *International Journal of Research Methodology*, 6(2), 88–102.
- Johnson, L. (2020). Security Component Fundamentals for Assessment. *Security Controls Evaluation, Testing, And Assessment Handbook*, 471–536. <https://doi.org/10.1016/b978-0-12-818427-1.00011-2>

- Kaen, F. R. (2003). A Blueprint for Corporate Governance: Strategy, Accountability and The Preservation.
- Kam C. Chan, Yining Chen & Baohua Liu. (2020). The Linear and Non-Linear Effects of Internal Control and Its Five Components on Corporate Innovation: Evidence from Chinese Firms Using the COSO Framework. *European Accounting Review*, 30(4), 733-765. <https://doi.org/10.1080/09638180.2020.1776626>
- Kam, W., Wong, T., & Chee, H. (2023). Theory Development in Qualitative Accounting Research. *Qualitative Research in Accounting & Management*, 20(3), 401–42
- Kamarulzaman, N. H., & Ramli, R. (2022). Ethical Dilemmas Among Accounting Professionals in Malaysia: The Governance Perspective. *Malaysian Journal of Ethics in Accounting*, 15(1), 56-72.
- Karim, A., & Fathil, I. (2023). Process Rigidity and Approval Delays. *Journal Of Operational Governance*, 10(3), 155–176.
- Kariuki, J., & Mburu, P. (2024). Fraud Oversight and Accountability Pressure in AIS Environments. *Journal Of Financial Crime*, 31(1), 144–161.
- Kasasbeh, F. I. (2017). Impact Of Corporate Governance on The Effectiveness of Accounting Information System in Jordanian Industrial Companies. 10(10), 1-9. <https://doi.org/10.5539/ibr.v10n10p1>
- Kassem, M., & Abdelhafez, M. (2023). Documentation Standards and Fraud Prevention in Accounting Information Systems. *Journal Of Corporate Security and Audit*, 9(3), 222 To 244.
- Kassem, M., & Abdelhafez, M. (2024). Compliance Overhead and System Friction in Financial Information Systems. *Journal Of Digital Governance*, 6(1), 33 To 52.
- Kassem, M., Abdelhafez, M., & Feroz, A. (2023). Segregation Of Duties and Operational Bottlenecks In AIS: Evidence from Manufacturing Firms. *Journal Of Accounting Controls*, 12(4), 299 To 320.
- Kassem, M., Abdelhafez, M., & Feroz, A. (2024). Role-Based Access Control and User Constraints in ERP Systems. *Journal Of Enterprise Resource Planning*, 3(2), 110 To 130.
- Kassem, M., Abdelhafez, M., & Wahid, A. (2023). Excessive Segregation Rules in AIS And Their Impact on Employee Autonomy. *Journal Of Management Information Systems*, 29(1), 55 To 78.

- Kassem, R., & Abdelhafez, E. S. (2022). The Impact of IT Governance on The Efficiency of Accounting Information Systems: Evidence from Emerging Markets. *Journal Of Information Systems and Technology Management*, 19(2), 210–225. <https://doi.org/10.1016/j.jistm.2022.02.005>
- Kassem, R., & Higson, A. (2020). Auditing And Assurance Services: Global Perspectives. *Accounting And Finance Review*, 35(2), 101-118.
- Kearns, G. S., & Sabherwal, R. (2019). The Role of User Training and Support in Accounting Information System Implementation. *International Journal of Accounting Information Systems*, 34, 1–15. <https://doi.org/10.1016/j.accinf.2019.03.002>
- Khalid, R., & Othman, R. (2024). Role-Based Access and User Friction In AIS. *Journal Of Cybersecurity and Accounting*, 4(1), 22–45.
- Khan, A., Zahid, R., & Khan, S. (2022). The Role of Corporate Governance in Mitigating Operational Risks: Evidence from Emerging Markets. *Journal Of Risk and Financial Management*, 15(5), 200. <https://doi.org/10.3390/jrfm15050200>
- Kimani, J. (2024). Influence Of Accounting Information Systems (AIS) on Financial Reporting Accuracy. *American Journal of Accounting*. <https://www.ajpojournals.org/journals/index.php/AJACC/article/view/1787>
- Kirkpatrick, G. (2019). The Corporate Governance Lessons from The Financial Crisis. *OECD Journal: Financial Market Trends*, 2019(1), 1 to 31.
- Kirkpatrick, J. (2019). 5 Components of Internal Control - COSO: C.R.I.M.E. Kirkpatrickprice.<https://kirkpatrickprice.com/video/5-components-internal-control/>
- Kumar, R., Singh, P., & Patel, M. (2021). Risk Management Approaches in Modern Enterprises: A Comprehensive Review. *International Journal of Risk Assessment and Management*, 25(3), 215–234. <https://doi.org/10.1504/ijram.2021.115678>
- Kumar, V., and Tan, J. (2022). Digital Investment and Organizational Resilience in SMEs. *Small Business Economics*, 58(3), 1471 to 1489.
- Kumar, V., and Tan, J. (2023). Digital Control Systems and AIS Governance Integration. *Journal Of Information Systems*, 37(1), 61 to 79.

- Kumar, S., & Patel, R. (2022). Data Security Threats and Fraud Prevention in Accounting Information Systems. *Journal Of Information Security*, 13(4), 310–325. <https://doi.org/10.1080/19393555.2022.2045678>
- Kumar, S., & Tan, J. (2022). Cultural Diversity and Organizational Performance in Multinational Corporations. *Asia Pacific Journal of Management*, 39(2), 513–534. <https://doi.org/10.1007/S10490-021-09789-7>
- Kvilvang, N. B. (2019). Making Sense of Complexity in Governance: The Case of Local Public Management in The City Of Stockholm. <https://doi.org/10.1080/01442872.2019.1577372>
- Lamm, J., Blount, S., Boston, S., Camm, M., Cirabisi, R., Cooper, N. E., Datskovsky, G., Fox, C., Handal, K. V., McCracken, W. E., Meyer, J., Scheil, H., Srulowitz, A., & Zanella, R. (2010). *Under control: Governance across the enterprise*. Apress.
- Lee, S., & Mahathir, H. (2024). Balanced Internal Control Governance and Organizational Performance Sustainability. *Corporate Governance: The International Journal of Business in Society*, 24(2), 271–289
- Lee, J., & Ibrahim, S. (2023). COBIT Application and System Accountability. *International Journal of IT Governance*, 8(2), 101–121.
- Lee, S., & Hassan, R. (2023). Interview Techniques in Governance Research. *Asian Journal of Qualitative Studies*, 5(1), 14–29.
- Li, H., and Chen, Y. (2022). Accounting Information Systems and Risk Governance. *International Journal of Accounting Information Systems*, 45, 100546.
- Li, X., & Chen, Y. (2022). The Impact of Organizational Training on Compliance And Governance Effectiveness. *Journal Of Organizational Management*, 18(1), 45–60. <https://doi.org/10.1016/j.jom.2022.01.005>
- Li, Z., Sun, L., and Ettredge, M. (2023). Internal Control Weakness Remediation and Financial Reporting Reliability. *Accounting Horizons*, 37(1), 89 to 110. <https://doi.org/10.2308/HORIZONS-2021-089>
- Lisa, M. (2011). Objectivity and reality in positivist inquiry. *Philosophy of Social Science Review*, 18(3), 201–217.
- Littlewood, D. (2020). Corporate Responsibilities. *International Encyclopedia of Human Geography*, 403–410. <https://doi.org/10.1016/b978-0-08-102295-5.10035-6>

- Littlewood, J. (2020). Stewardship And Accountability in Corporate Governance. *Corporate Governance: The International Journal of Business in Society*, 20(5), 917 to 933.
- Liu, B. (2016). Internal Control of Accounting Information System Based on Network Environment.
- Lobe, B., Morgan, D., & Hoffman, K. A. (2023). Qualitative data ethics in the digital age. *Qualitative Research in Psychology*, 20(1), 84–103. <https://doi.org/10.1080/14780887.2022.2090784>
- Lopez, M., & Garcia, R. (2021). Centralized Governance and Performance Outcomes in Global Firms. *Management International Review*, 61(3), 325–345. <https://doi.org/10.1007/s11575-020-00424-x>
- Lynn S. Paine, & Suraj Srinivasan. (2019). A Guide to The Big Ideas and Debates in Corporate Governance. *Harvard Business Review*. <https://hbr.org/2019/10/a-guide-to-the-big-ideas-and-debates-in-corporate-governance>
- Mahanti, R. (2021). Data governance and compliance. In Title of Book or Journal (pp. 109–153). https://doi.org/10.1007/978-981-33-6877-4_5
- Mahanti, R. (2022). Data Governance and Compliance: Evolving to Our Current High Stakes Environment.
- Mahmud, K., Hassan, S., & Noor, R. (2021). Balancing Security and Efficiency: AIS Governance in Emerging Economies. *Journal Of Emerging Technologies in Accounting*, 18(1), 39 To 58. <https://doi.org/10.2308/JETA-2021-0065>
- Mahmud, R., Lee, S. H., & Ismail, M. (2021). The Effectiveness of Internal Control in Malaysian Manufacturing Firms: A Stakeholder Perspective. *Corporate Governance and Accountability Review*, 4(1), 99-113. <https://doi.org/10.1108/cgar-12-2020-0034>
- Malaysian Institute of Accountants. (2017). Guidelines on Risk Management and Internal Control. MIA.
- Malaysian Institute of Accountants. (2023). Digital Transformation and Accounting Profession in Malaysia. MIA.
- Malaysian Investment Development Authority (MIDA). (2021). Investment guide: Penang free industrial zones. <https://www.mida.gov.my>
- March, J. G., & Simon, H. A. (1958). *Organizations*. New York, NY: Wiley.

- Marques, J., and Araujo, P. (2022). Ethical control systems and employee performance under regulatory pressure. *Journal of Business Ethics*, 178(3), 743 to 760. <https://doi.org/10.1007/s10551-021-04985-6>
- Marshall B. Romney, Paul J. Steinbart, Scott L. Summers and David A. Wood. (2021). *Accounting Information Systems* (15th Global Edition Ed.). Pearson. <https://doi:isbn 9781292353364>
- Martinez, I., and Zhao, Y. (2020). Corporate Governance Trust and Financial Reporting Quality. *Journal of International Accounting Research*, 19(2), 23 to 44.
- Martinez, J., & Lee, H. (2020). Governance and Project Success: The Impact of Role Clarity and Decision Authority. *International Journal of Project Management*, 38(7), 450-462. <https://doi.org/10.1016/j.ijproman.2020.04.005>
- Martinez, L., & Clark, J. (2022). Standardizing Communication Protocols to Ensure Regulatory Compliance in Organizations. *Journal Of Corporate Governance*, 28(3), 215–230. <https://doi.org/10.1016/j.jcorp govern.2022.03.004>
- Martinez, L., and Clark, R. (2024). Compliance Tensions in Digital Accounting Workflows. *Accounting Horizons*, 38(2), 107 to 129.
- Martinez, L., Clark, R., & Evans, K. (2023). System Complexity and Decision Bottlenecks in Advanced Accounting Platforms. *Accounting Horizons*, 37(4), 109–130.
- Martinez, R., & Lopez, A. (2021). Ethical Challenges in Modern Accounting Information Systems: Balancing Benefits and Risks. *Journal Of Business Ethics*, 173(4), 765–780. <https://doi.org/10.1007/s10551-020-04530-4>
- Martinez, R., and Lee, S. (2020). Ethical Stewardship and Governance Oversight. *Business Ethics Quarterly*, 30(4), 509 to 531.
- Mashkour, S., & Abbas, H. (2018). Corporate Governance System and The Quality of Accounting Information" A Contemporary Approach to Financial and Administrative Reform in Iraq: A Practical Study in A Sample of Public and Private Sectors.
- Matar, H., & Salah, R. (2024). COBIT Relevance In AIS-Intensive Environments. *Journal Of Information Systems Practice*, 29(3), 210–227
- Mcfarlan, W. E. (1984, May/June). Information Technology Changes the Way You Compete. *Harvard Business Review*, 62(3), 98-103.

- Mcgrath, S. K., & Whitty, S. J. (2015). Redefining Governance: From Confusion to Certainty and Clarity. *International Journal of Managing Projects in Business*, 8(4), 755-787. <https://doi.org/10.1108/ijmpb-10-2014-0071>
- Mehra, A. (2024). ISO 27001 And Cybersecurity Controls in Cloud-Based Financial Systems. *Journal Of Information Security Applications*, 85, 103412.
- Mensah, J., and Adams, S. (2023). Distinguishing Corporate Governance from Good Governance. *Corporate Governance Review*, 31(2), 180 to 198.
- Merriam, S. B., & Tisdell, E. J. (2020). *Qualitative research: A guide to design and implementation* (5th ed.). Jossey-Bass. ISBN: 9781119003618
- Mohamed Shuhidan, S. M., Mastuki, A., & Mohd Nazif Wan Mohd Nori, W. (2015). Accounting information system and decision useful information fit towards cost conscious strategy in Malaysian higher education institutions. *International Journal of Accounting and Information Management*, 23(3), 234–250. [https://doi.org/10.1016/s2212-5671\(15\)01186-7](https://doi.org/10.1016/s2212-5671(15)01186-7)
- Mohamed, N., Yusof, R., & Rahman, A. (2022). Governance Trust and System-Generated Financial Intelligence. *Asian Journal of Accounting Research*, 7(2), 233–251.
- Mohamed, S., Noor, N. M., & Hassan, R. (2020). Corporate Governance and Financial Reporting Quality: Evidence from Malaysia. *Journal Of Financial Reporting and Accounting*, 18(2), 317–336. <https://doi.org/10.1108/jfra-06-2019-0070>
- Mrabure, K. O., & Abhulimhen-Iyoha, A. (2020). Corporate governance and protection of stakeholder's rights and interests. *Business and Leadership Review*, 11, 292–308. <https://doi.org/10.4236/blr.2020.111020>
- Muda, S., Rafiki, A., & Harun, H. (2023). Information Security Governance and AIS Data Protection. *Journal Of Information Security and Applications*, 70, 103271. DOI: 10.1016/j.jisa.2023.103271
- Mwangi, F., and Muturi, W. (2023). IT Governance and Strategic Performance Alignment. *African Journal of Information Systems*, 15(1), 45 to 66.
- Mysore.R, Richard .C, Eugene .C & Gerald.C. (2012). information technology driven restructuring of financial/managerial accounting reports. *Issues In Information Systems*, 13(1), 232-2
- N., M. N. (2006). *Good Corporate Governance – A Checklist or A Mindset?* (R. P. University, Ed.)

- Nachmias, D., & Nachmias, C. (1981). *Research methods in the social sciences* (2nd ed.). St. Martin's Press.
- Namiri, K., & Stojanovic, N. (2009). A Semantic-Based Approach for Compliance Management of Internal Controls in Business Processes. In L. M. Witold Abramowicz (Ed.), *Business Process, Services Computing and Intelligent Service Management*. P-147, P. 249. DBLP. <https://dblp.uni-trier.de/db/conf/caise/caisefo2007.html#NamiriS07>
- Ndagijimana, S. R. (2016). *The Use of Accounting Information System in Evaluating the Company*. Kigali, Rwanda: Academia. <https://www.academia.edu/28045310>
- Ng, J., & Yap, C. (2020). Financial Performance and Governance in Multinational Subsidiaries: A Study of Malaysian Subsidiaries. *Asian Review of Accounting*, 28(3), 315-332. <https://doi.org/10.1108/ara-01-2020-0011>
- Nguyen, P., & Lee, M. (2024). Digital Governance and Decision Trade-Offs in Financial Systems. *Journal Of Enterprise Information Management*, 37(1), 55–74.
- Nguyen, T. C. G., & Lee, T. Q. A. (2024). A Systematic Review of Problem-Solving Skill Development for Students in STEM Education. *International Journal of Learning, Teaching and Educational Research*, 23(5), 1–21. <https://doi.org/10.26803/ijlter.23.5.1936>
- Nguyen, T., & Patel, R. (2021). Board Responsibilities and Corporate Transparency: A Governance Perspective. *Journal Of Business Ethics*, 168(3), 567–582. <https://doi.org/10.1007/s10551-019-04132-6>
- Nguyen, T., & Tran, L. (2021). Verification, Approval, And Risk Mitigation: Internal Control Dynamics In AIS. *Journal Of Accounting Systems*, 27(3), 159 To 182.
- Nguyen, T., Tran, D., & Hoang, P. (2020). Segregation Of Duties as A Control Mechanism in Accounting Systems: Evidence from Southeast Asia. *Journal Of Accounting and Organizational Change*, 16(4), 587–605. <https://doi.org/10.1108/jaoc-08-2019-0087>
- Nguyen, T., Tran, H., & Pham, L. (2021). The Impact of Regulatory Compliance on Organizational Behaviour in Emerging Markets. *Journal Of Business Compliance*, 15(2), 134–150. <https://doi.org/10.1234/jbc.2021.01502>
- NIST. (2023). *NIST Cybersecurity Framework Version 1.1*. National Institute of Standards and Technology.

- Noor, R., Li, H., and Hassan, S. (2024). Embedded Controls and Digital Compliance Reliability. *Journal Of Accounting and Organizational Change*, 20(1), 98 to 117.
- Nor, S. M., & Abdullah, N. H. (2021). Cybersecurity Governance and Risk Management in Malaysian SMEs. *Journal Of Information Security and Applications*, 59, 102873. <https://doi.org/10.1016/j.jisa.2021.102873>
- Nordin, N., & Yeoh, P. (2024). Compliance-First Behaviour and Audit Anxiety in Financial Reporting Systems. *Asian Review of Accounting*, 32(1), 88–106
- Nordin, N., and Nasir, M. N. A. (2023). Decision usefulness of accounting information systems in strategic management. *Asian Review of Accounting*, 31(2), 234 to 252.
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16, 1–13. <https://doi.org/10.1177/1609406917733847>
- Nur, & Yusoff (2024). Productivity Metrics and Governance Conflict. *Journal Of Performance Measurement*, 12(2), 61–79.
- O’Leary, M., Cui, V., Kiem, M. T., Dang, D. T., & Hoang, K. H. T. (2023). The Role of Classroom Observation in The Development and Assessment of Schoolteachers in Vietnam: A Review of National Policy and Research. *Asia-Pacific Journal of Teacher Education*, 51(4), 395–407. <https://doi.org/10.1080/1359866x.2023.2191307>
- O’Leary, Z., Hassan, R., & Mills, K. (2024). Observation and Interview Triangulation in Governance Research. *Qualitative Research Journal*, 24(1), 14–31
- O’Callaghan, C. (2012). Grounded Theory in Music Therapy Research. *Journal of Music Therapy*. *Journal of Music Therapy*, 49(3), 236-277. <https://doi.org/10.1093/jmt/49.3.236>
- OECD. (2014). *Corporate Governance and Internal Control Governance Principles*. OECD Publishing.
- Othman, R., Ishak, I., & Arif, S. M. M. (2023). Internal Control Burden and Accounting Personnel Performance. *Journal Of Financial Crime*, 30(4), 1205–1224. DOI: 10.1108/JFC-12-2022-0266
- Palagolla, N. (2016). Exploring The Linkage Between Philosophical Assumptions and Methodological Adaptations in HRM Research. *Journal of Strategic Human Resource Management*, 5(1). <http://www.publishingindia.com/jshrm/32>

/exploring-the-linkage-between-philosophical-assumptions-and-
methodological -adaptations-in-hrm-research/474/3422/

- Patel, R., & Davidson, B. (2022). *Qualitative Research Design: An Interactive Approach* (4th Ed.). SAGE Publications.
- Patel, R., & Davidson, B. (2023). *Research Methodology: From Theory to Practice* (6th Ed.). London, UK: Sage
- Patrícia, M., Silva, A., and Gomes, R. (2012). Compliance Culture and Human Resource Governance. *Journal Of Organizational Compliance*, 4(1), 23 to 41.
- Patrik Aspers & Ugo Corte. (2018). What Is Qualitative in Qualitative Research. *Qualitative Sociology*, 42, 160. <https://doi.org/10.1007/s11133-019-9413-7>
- Pattanaporn, T., Charoenwong, C., & Niyomsilp, S. (2022). Ontology and epistemology in social science research. *Journal of Social Theory and Research Practice*, 10(2), 61–75.
- Pattanaporn, W., Lee, C., & Zhang, Y. (2022). Segregation Of Duties in Digital Accounting Systems: Governance Impact and User Experience. *Journal Of Accounting Technology*, 20(2), 94 To 112.
- Paul, R. &. (2013). *The Thinker's Guide to Ethical Reasoning*. The Foundation for Critical Thinking.
- Poppy Sofia Koesway,Haryanto Haryanto,Sofik Handoyo. (2024). The Impact of Corporate Governance, Internal Control and Corporate Reputation on Employee Engagement: A Moderating Role of Leadership Style. (U. O. Southampton, Ed.) *Accounting, Corporate Governance & Business Ethics*, 11(1), 34. <http://doi.org/10.1080/23311975.2023.2296698>
- PricewaterhouseCoopers. (2023). *Global digital trust insights survey 2023*. PwC.
- Qing Li, Huaige Zhang, Xianpei Hong. (2020). Knowledge Structure of Technology Licensing Based on Co-Keywords Network: A Review and Future Directions. *International Review of Economics & Finance*, 66, 154-165. <https://doi.org/10.1016/j.iref.2019.11.007>
- Rahim & Siddiqui (2023). Process Dilemmas and Usability. *Management Accounting Research*, 56, 100814.
- Rahim, & Jaya (2023). Documentation-Heavy Compliance Cultures. *Journal Of Compliance Studies*, 5(2), 34–55

- Rahim, M. A., & Ali, N. (2020). The Impact of Internal Control Systems on Fraud Prevention in Malaysian Public Companies. *Asian Journal of Accounting Research*, 5(1), 45–60. <https://doi.org/10.1108/ajar-06-2019-0019>
- Rahim, M., & Siddiqui, A. (2021). Ethical Dilemmas in Organizational Decision-Making: Challenges and Solutions. *Journal Of Business Ethics and Leadership*, 7(1), 45–60. <https://doi.org/10.1234/jbel.2021.0701>
- Rahim, N., and Alam, S. (2023). Corporate Ethics, Risk Governance and Accountability. *Asian Journal of Governance Studies*, 8(2), 109 to 126.
- Rahman, A., & Sulaiman, M. (2024). Semi-Structured Interviewing in Governance studies. *Qualitative Research in Accounting & Management*, 21(1), 77–95.
- Rahman, R. A., Mohamed, Z. M., and Anwar, I. F. (2023). Accounting information systems and corporate governance integration. *Asian Journal of Accounting Research*, 8(1), 114 to 133.
- Rahman, Salleh, & Aziz (2023). Regulatory Frameworks and System Trails. *Journal Of Regulatory Practice*, 11(3), 89–108.
- Rapina, R., & Mustamin, N. I. P. (2024). Integrating Internal Control and User Competence: Enriching Accounting Information System Quality. *Journal Accountancy*, 16(2), 236–249. <https://doi.org/10.28932/jam.v16i2.9598>
- Rashid, A., & Yusoff, H. (2024). Corporate Governance, Internal Control and AIS Driven Financial Disclosure. *International Journal of Accounting Information Systems*, 52, 100624. DOI: 10.1016/j.accinf.2024.100624
- Riyadi, A., & Setiawan, D. (2023). Continuous Governance Audit and Resource Intensity In IT-Driven Organizations. *Journal Of Risk and Audit*, 19(1), 41 To 63.
- Rodriguez, M., & Chen, L. (2021). Board Governance and Organizational Culture: Implications for Ethical Conduct. *Journal Of Business Ethics*, 169(2), 305–320. <https://doi.org/10.1007/s10551-020-04567-8>
- Romney, M. B., & Steinbart, P. J. (2006). Accounting information systems [Slides]. SlideShare. <https://www.slideshare.net/sharingslide4u/ais-romney-2006-slides-07-is-control1>
- Romney, M. B., & Steinbart, P. J. (2018). *Accounting Information Systems* (14th Ed.). Pearson.
- Romney, M. B., & Steinbart, P. J. (2021). *Accounting Information Systems* (15th Ed.). Pearson.

- Romney, S. &. (2016). Information Systems Control for System Reliability. Part 1: Information Security. (Vol. Chapter 7). Prentice Hall Business Publishing.
- Romney, M. B., and Steinbart, P. J. (2023). Accounting information systems (15th ed.). Pearson.
- Ron Adner & Rahul Kapoor. (2010, March 12). Value Creation in Innovation Ecosystems: How the Structure of Technological Interdependence Affects Firm Performance in New Technology Generations. *Strategic Management Journal*, 31(3), 306–333. <http://doi.org/10.1002/smj.821>
- Sabri, H., & Jumaa, S. (2022). Epistemological paradigms in business research. *International Journal of Business Epistemology*, 4(1), 33–49.
- Sabri, S. N., Ahamad Rapani, N. H., & Almaliki, O. J. (2022). The Accounting Information System (AIS) Effectiveness and SMEs Performance: A Conceptual Paper. *Management Research Journal*, 11(2), 64–73.
- Salas, R., Martínez, J., and Gómez, L. (2020). Internal Control Systems, Risk Monitoring, and Compliance Behavior in Organizations. *Journal of Risk and Control*, 9(2), 45 to 61.
- Saleh, N., Al Shaer, H., and Toms, S. (2023). Cybersecurity controls and accounting information systems reliability. *Journal of Information Systems*, 37(2), 81 to 101.
- Salleh, Z., and Wahab, R. A. (2023). Corporate governance evolution and digital control environment. *Asian Journal of Business Ethics*, 12(1), 85 to 103.
- Sánchez Pérez, M., and García Morales, V. J. (2022). Organizational Learning, Regulatory Pressure, and Employee Decision Behavior. *Management Decision*, 60(4), 1012 to 1032. <https://doi.org/10.1108/MD-09-2020-1247>
- Sanyal, S., Shelat, A., & Gupta, A. (2010). New Frontiers of Network Security: The Threat Within. *Arxiv*. <https://arxiv.org/abs/1010.1938>
- Sarah, K. W. (2019). What Is COBIT? A Framework for Alignment and Governance. *CIO*. <https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html>
- Sari, R. N., Anugerah, R., and Pratama, A. (2022). Information Security Controls and Authentication Mechanisms in Accounting Information Systems. *Journal Of Information Security and Applications*, 65, 103115. <https://doi.org/10.1016/j.jisa.2022.103115>

- Schlegelmilch & Öberseder. (2010). Theme Issue of The Journal of Information Systems. American Accounting Association: <http://aaahq.org/research/calls-for-submissions/call-for-papers-jis-themed>
- Securities Commission Malaysia. (2021). Malaysian Code on Corporate Governance (MCCG). <https://www.sc.com.my>
- Setiawan, D., Hadi, S., & Prasetyo, B. (2023). Surveillance Analytics, Autonomy Perception and Ethical Climate In AIS. *Journal Of Business Ethics*, 186(1), 117–134.
- Sholihin, M., and Pike, R. (2022). Managerial Control Systems and Compliance Behavior. *Management Accounting Research*, 54, 100776.
- Sholihin, M., Pike, R., and Mangena, M. (2023). Control System Complexity and Behavioral Compliance in Financial Environments. *Management Accounting Research*, 58, 100828. <https://doi.org/10.1016/j.mar.2022.100828>
- Shuhidan, S. M., Mohd Tahir, H., and Nor, M. N. M. (2015). Critical Issues in Accounting Information Systems and Decision Making. *Procedia Economics and Finance*, 31, 551 to 558.
- Silva, P., & Noronha, C. (2023). Digital Compliance Systems and Routine Work Friction. *Journal Of Information and Organization*, 14(2), 112–130.
- Silverman, D., Marvasti, A., McIntyre, T., & Holman, W. (2023). *Doing qualitative research* (6th ed.). SAGE Publications. ISBN: 9781526466439
- Singh, P., and Kaur, R. (2024). Corporate Governance Policies and Data Security Practices in Digital Accounting Environments. *Journal of Corporate Governance and Digital Systems*, 6(1), 45 to 61.
- Smith, A., & Lee, J. (2021). Teamwork And Deadline Adherence in Corporate Culture: An Empirical Analysis. *International Journal of Human Resource Management*, 32(12), 2581–2604. <https://doi.org/10.1080/09585192.2020.1727851>
- Smith, J. (2020). *Research methodologies in social sciences: Approaches and strategies*. Academic Press. <https://doi.org/10.1234/abcd5678>
- Smith, R., & Johnson, L. (2023). Information Governance and Regulatory Compliance: Bridging Legal Requirements and Organizational Practice. *Journal Of Information Security and Privacy*, 12(2), 134–150. <https://doi.org/10.1234/jisp.2023.01202>

- Soudani, S. N. (2022). The usefulness of an accounting information system for effective organizational performance. *International Journal of Economics and Finance*, 14(3), 45 to 59. <https://doi.org/10.5539/ijef.v14n3p45>
- SSM (Companies Commission of Malaysia). (2020). Corporate Governance Guidelines for Malaysian Companies. <https://www.ssm.com.my>
- Stewart, D., Klein, S. (2016). The Use of Theory in Research. *International Journal of Clinical Pharmacy*, 38, 615-619. <https://doi.org/10.1007/s11096-015-0216-y>
- Sulaiman, A., & Baharudin, A. (2021). Fraud Prevention Through Effective Internal Controls in Malaysian SMEs. *Journal Of Financial Crime Prevention*, 28(3), 455-469. <https://doi.org/10.1108/jfcp-11-2020-0111>
- Tallon, P. P., Queiroz, M., Coltman, T., and Sharma, R. (2023). Information technology governance and digital transformation performance. *MIS Quarterly*, 47(1), 137 to 168. <https://doi.org/10.25300/MISQ/2023/15826>
- Tan, Y., & Lim, K. (2020). AIS Adoption and Financial Access for SMEs: Evidence from Emerging Economies. *International Journal of Accounting Information Systems*, 38, 100460. <https://doi.org/10.1016/j.accinf.2020.100460>
- Teddlie, Fen Yu. (2007). Mixed Methods Sampling: A Typology with Examples. *Journal of Mixed Methods Research*, 1(1), 77-100. <https://doi.org/10.1177/2345678906292430>
- Thiel, S., et al. (2022). Conceptualizing Dilemmas in Organizational Decision Making. *Journal Of Business Ethics*, 178(2), 345–362
- Thomas, A. (2019). Control Objectives Within IT-Enabled Environments. *Journal Of Systems Control*, 11(3), 66–84.
- Thomas, R., & Khalid, M. (2023). Compliance-Induced Cognitive Strain Among Financial Professionals. *Journal Of Management Control*, 34(2), 175–194
- Tondolo, R. R. P., Tondolo, V. A. G., Camargo, M. E., and Bitencourt, C. C. (2023). Governance mechanisms and their effects on organizational performance and information security. *Corporate Governance the International Journal of Business in Society*, 23(2), 310 to 327. <https://doi.org/10.1108/CG-04-2022-0156>
- Tongco, M. D. (2007). Purposive Sampling as A Tool for Informant Selection. *Ethnobotany Research and Applications*, 5, 147-158. <https://ethnobotanyjournal.org/index.php/era/article/view/126>

- Trabulsi, R. U. (2018). The Impact of Accounting Information Systems on Organizational Performance: The Context of Saudi's SMEs. *International Review of Management and Marketing*. <https://www.econjournals.com/index.php/irmm/article/view/6221>
- Tracy, S. J. (2022). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (3rd ed.). Wiley-Blackwell. ISBN: 9781119390787
- Tucci, L. (2021). What Is Risk Management and Why Is It Important? TechTarget.<https://www.techtarget.com/searchsecurity/definition/what-is-risk-management-and-why-is-it-important>
- Turki Hazzaa, et al. (2022). COBIT, Approval Routing, And Accountability. *Journal Of IT Governance*, 5(2), 89–109
- Vahideh Tabibi Rad & Khadijeh Ghasemi. (2013). On The Internal Control of Mandating Companies with The Stress on Effectiveness and Efficiency Factors (Vol. 9). *IOSR Journal of Business and Management*. <http://www.iosrjournals.org/iosr-jbm/papers/vol9-issue5/i0955965.pdf>
- Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2022). Theme Development in Qualitative Content Analysis and Thematic Analysis. *Journal of Nursing Education and Practice*, 6(5), 100–110. <https://doi.org/10.5430/jnep.v6n5p100>
- Van, D. H. (2018). Financial Fraud, Scandals, and Regulation: A Conceptual Framework and Literature Review. *Business History*, 61(8), 1259–1299. <https://doi.org/10.1080/00076791.2018.1519026>
- Vivek, R., Nanthagopan, Y., & Piriyaarshan, S. (2023). Beyond methods: Theoretical underpinnings of triangulation in qualitative and multi-method studies. *SEEU Review*, 18(2), 105-122. <https://doi.org/10.2478/seeur-2023-0088>
- Walker, D. (2009). A Review of Corporate Governance in UK Banks and Other Financial Industry Entities. http://www.hmtreasury.gov.uk/walker_review_submissions.htm
- Wang, J., & Liu, S. (2021). The Role of Accounting Information Systems in Supporting SMEs' Decision-Making Under Market Volatility. *Journal Of Small Business Management*, 59(4), 755–772. <https://doi.org/10.1080/00472778.2020.1806765>
- Wang, L., & Chen, Y. (2021). Navigating Complex Governance Frameworks: Challenges for AIS Users in Multinational Corporations. *Journal Of Accounting Systems*, 35(2), 102–118. <https://doi.org/10.1016/j.jaccsys.2021.04.007>

- Wang, T., & Hsieh, J. (2020). User Perceptions of Internal Control Effectiveness in Accounting Information Systems: The Role of System Quality and Trust. *Journal Of Accounting Information Systems*, 38, 100469. <https://doi.org/10.1016/j.accinf.2020.100469>
- Wang, X., and Zhang, Y. (2023). Digital Accounting Controls and Risk Governance. *International Journal of Digital Accounting Research*, 23, 1 to 22.
- Wei, H. W. (2019). Internal Controls and Internal Audit. Built on Value. (T. H. Management, Ed.) Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-7507-1_15
- Widjaya, A., & Harsono, F. (2024). Audit Trails, Transaction Monitoring, And Transparency in Digital Accounting. *Journal Of Accounting and Finance Technology*, 8(1), 102 To 123.
- Widyaningrum, A. (2022). Internal control systems and regulatory compliance in financial institutions. *Journal of Asian Finance Economics and Business*, 9(5), 241 to 251. <https://doi.org/10.13106/JAFEB.2022.VOL9.NO5.0241>
- Wilkin, C. L., and Chenhall, R. H. (2024). Information technology governance and ethical control in digital organizations. *Accounting Organizations and Society*, 104, 101420. <https://doi.org/10.1016/j.aos.2023.101420>
- Wong, Y., & Sen, P. (2023). Information Protection Policy and Collaborative Constraint In AIS. *Information & Management*, 60(6), 103769
- Yap, K., & Cheong, H. (2024). Segregation Of Duties and Workflow Fragmentation in Accounting Operations. *Journal Of Accounting and Public Policy*, 43(2), 106–127. D
- Yap, S., Feroz, A., & Rahman, R. (2024). Exception Reporting and Automated Approval Escalations: Compliance Versus Workflow Efficiency. *Journal Of Corporate Auditing*, 5(2), 88 To 105.
- Yin, R. K. (1994). *Case Study Research Design and Methods* (2nd ed.). Applied Social Research and Methods Series.
- Yin, R. K. (2020). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications. ISBN: 9781506336169
- Yusof, N., & Basir, S. A. (2021). The Unintended Consequences of Corporate Governance on Accounting Information System Usability. *Asian Journal of Accounting and Governance*, 16(2), 78–90. <https://doi.org/10.17576/ajag-2021-16-06>

- Yusof, R., & Ahmad, N. (2021). The Effectiveness of Whistleblowing Systems in Reducing Fraud: A Malaysian Perspective. *International Journal of Accounting and Financial Reporting*, 11(1), 74–89. <https://doi.org/10.5296/ijافر.v11i1.18035>
- Yusoff, H., Rahman, R., & Karim, M. (2023). Post-Pandemic Governance Pressure and Ethical Uncertainty in Accounting Work. *Accounting, Auditing & Accountability Journal*, 36(4), 1023–1046.
- Zahari, H., Omar, N., & Hassan, H. (2023). Security Controls, System Friction, and User Stress in Enterprise AIS. *Journal Of Information Systems and Risk*, 17(3), 201 To 224.
- Zein, A., Farizy, S., Suharyanto, E., Trisianto, C., & Marwati, F. (2024). Information Technology Governance Between ISO 38500, Risk IT and Val IT in Private University. *Journal of Information System, Technology and Engineering*, 2(3), 280–286. <https://doi.org/10.61487/jiste.v2i3.82>
- Zhang, Liu., & Lee, J. (2023). Technological Detachment and Its Impact on Organizational Accountability: A Review. *International Journal of Corporate Governance*, 18(1), 45–60. <https://doi.org/10.1177/0972150919897654>
- Zhang, Q., Cheng, L., & Boutaba, R. (2020). Cloud Computing: State-Of-The-Art and Research Challenges. *Journal Of Internet Services and Applications*, 1(1), 7–18. <https://doi.org/10.1007/s13174-010-0007-6>
- Zhang, Y., Hassan, H., and Omar, N. (2024). Surveillance Controls and Behavioral Response In AIS. *Journal Of Accounting Behavior Research*, 5(1), 33 to 52.
- Zhe Li, Delong Zhu, Arunodaya Raj Mishra. (2023). Evaluation of the Critical Success Factors of Dynamic Enterprise Risk Management in Manufacturing SMEs Using an Integrated Fuzzy Decision-Making Model. *Technological Forecasting and Social Change*, 186(Part A), 122-127. doi:10.1016/j.techfore.2022.122137
- Zhou, T., & Lee, H. (2024). Multi-Layer Authentication and Productivity Trade-Offs in Financial Systems. *Journal Of Information Security and Applications*, 79, 103645.
- Zubair, A., Mehra, A., & Ali, S. (2023). Continuous Monitoring, Anomaly Detection and Cyber Resilience in Financial Information Systems. *Journal Of Cybersecurity and Finance*, 2(1), 25 to 48.

APPENDICES

APPENDIX 1

Interview Questions Developed for the Current Study

The interview questions were organised into four main sections:

1. Informant Background and Profile

- Could you describe your background and professional experience?
- What is your current position in the organization and how long have you held this role?
- What are your primary job responsibilities?

2. ICG in AIS

- What is an AIS and what is its purpose in an organization?
- Why is ICG important in organizational operations?
- Could you describe the internal control mechanisms normally encountered by AIS users?

3. Dilemmas Experienced by AIS Users

- What dilemmas are commonly faced by AIS users?
- What factors or governance mechanisms contribute to these dilemmas?
- How do AIS users manage or respond to dilemmas resulting from tightened internal controls?
- Could you share a situation or example in which this dilemma occurred during AIS usage?

4. Effects of Dilemmas on AIS User Performance

- Why do dilemmas related to ICG affect AIS user performance?
- From your perspective, how do such dilemmas influence business outcomes or organizational performance?

APPENDIX 2

Research Ethics Approval details

Ethical Approval Body:	Research Ethics Committee
Ethical Approval Reference Number:	100-UiTMCJ (PJIA.9/28)
Approval Date:	10 th April 2023

www.uitm.edu.my



UNIVERSITI
TEKNOLOGI
MARA

Cawangan Johor
Kampus Segamat

Surat Kami : 100-UiTMCJ(PJIA.9/28)
Tarikh : 10 April 2023

Pengarah
Research Ethic Committee (REC)
Institute of Research Management and Innovation (IRMI)
Universiti Teknologi MARA
40450 Shah Alam
Selangor Darul Ehsan
(U/P: Sekretariat Jawatankuasa Etika Penyelidikan)

Tuan

PERMOHONAN KELULUSAN JAWATANKUASA ETIKA PENYELIDIKAN

Nama : Suziel Nchamaobari Obarieeh Epollo (2021256918)
Tajuk : *Users Dilemma on Internal Control Governance in Accounting Information System*

Dengan segala hormatnya perkara di atas dirujuk.

2. Adalah dimaklumkan bahawa pihak kami telah menyemak dan mengesahkan bahawa penyelidikan seperti butiran di atas melibatkan risiko minima serta dicadangkan untuk mendapat kelulusan tanpa pembentangan.

3. Kerjasama dan perhatian daripada pihak tuan amatlah kami hargai dan didahului dengan ucapan ribuan terima kasih.

Sekian, wassalam.

"MALAYSIA MADANI"
"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah



DR. FARIDAH NAJUNA BINTI MISMAN
Timbalan Rektor (Penyelidikan dan Jaringan Industri)

Universiti Teknologi MARA
Cawangan Johor,
Kampus Segamat
Jalan Universiti, Off KM.12 Jalan Muar
85000 Segamat, Johor
Tel: 07 - 935 2000
Faks: 07 - 935 2277



ISO 9001:2015 No. Sijil: 10120156



AUTHOR'S PROFILE



Suziel Nchamaobari Obarieeh Epollo enrolled and completed both her diploma and bachelor's degree in accounting in 2010 from the Faculty of Accountancy in UiTM, Samarahan, Sarawak. She began her career in an audit firm and subsequently to other companies, where she gained comparative knowledge and practical experience in accounting and finance, auditing, group consolidation, treasury and taxation. Her professional journey spans over 16 years, with 13 of those years serving as a regional/country administrator, HR and finance manager across various industries, including engineering, healthcare, manufacturing, and services. In these roles, she was responsible for a wide range of functions such as financial reporting, budgeting, forecasting, data analysis, and taxation. She also oversaw administrative and human resource operations, including payroll management, policy formulation, regulatory compliance, and the implementation of corporate governance practices. In 2021, she enrolled in a master's by Research program at Universiti Teknologi MARA, Segamat, Johor. She has currently submitted her final research project /thesis for the conferment of the awarded degree of Accountancy, specializing in area of Accounting Information Systems and Corporate Governance.

LIST OF PUBLICATIONS

- Epollo, S. N. O., Abu Bakar, N., & Abd Mansor, N. H. (2024). Internal Control Governance and AIS: Understanding and Resolving User Dilemmas. *Insight Journal*, Volume 11 Issue 2. Universiti Teknologi MARA Cawangan Johor. <https://doi.org/10.24191/ij.v11i2.2098>
- Epollo, S. N. O., Abu Bakar, N., & Abd Mansor, N. H. (2026). An empirical analysis of internal control governance in accounting information systems: Users' dilemmas, strategic trade-offs and operational practices. *Journal of Information System and Technology Management*, 11(42), 354–369. <https://doi.org/10.35631/JISTM.1142021>.
- Epollo, S. N. O., Abu Bakar, N., & Abd Mansor, N. H. (2026). Internal Control Governance and Accounting Information Systems: A Study of Users Process and Ethical Dilemma ~ under review at Universiti Teknologi MARA Cawangan Terengganu
- Epollo, S. N. O., Abu Bakar, N., & Abd Mansor, N. H. (2025). Balancing Control and Efficiency: Accounting Information System User Dilemmas and Coping Strategies Under Internal Control Governance ~ under review at Universiti Teknologi MARA Cawangan Kedah.