

Chapter 2 - LITERATURE REVIEW

2.1 Introduction

This chapter lays the theoretical and empirical groundwork for the research by providing an in-depth, analytical review of literature relevant to developing an intelligent document governance system.

The chapter begins by describing the specific operational environment of Swiss German University (SGU), the case study for this research. The context, including the university's people, processes, and technology, provides the critical lens through which all subsequent literature is reviewed. This ensures that the review is a targeted investigation, not a general survey, to identify the most relevant principles, frameworks, and technologies to solve SGU's specific challenges.

This review is structured into the following key sections to build a comprehensive understanding of the research domain:

- ***Theoretical Foundations:*** This section provides an overview of document and knowledge management principles and an in-depth examination of the ISO 15489 standard.
- ***Architectural and Governance Frameworks:*** A critical evaluation of enterprise architecture (TOGAF) and IT governance (COBIT) frameworks.
- ***Specific Governance Aspects:*** An examination of metadata governance (ISO 23081) and contract deadline management.
- ***Research Methodologies:*** A review of relevant paradigms, such as design science research (DSR), and methods for evaluating system usability.
- ***Enabling Technologies:*** An analysis of AI in document governance focusing on the Google Workspace ecosystem.
- ***Market Landscape:*** A comparative analysis of existing commercial and open-source document management system (DMS) solutions.

- ***Previous studies and research gaps:*** A critical analysis of prior work to identify the research gaps that this thesis aims to address.

2.2 Case Study Context: The Swiss German Univesity (SGU) Environment

To provide a practical context for the following literature review, this research focuses on the Swiss German University (SGU), a private higher education institution established in Indonesia in 2000. As the country's first international university, SGU has a long-standing commitment to quality assurance, initially demonstrated through ISO 9001 certification. Since 2012, the Indonesian higher education system has required the Sistem Penjaminan Mutu Internal (SPMI) under the Higher Education Law (Undang-Undang Republik Indonesia, 2012). Initially detailed in Permendikbud No. 62/2016, the framework was recently updated in Permendikbudristek No. 53/2023 (Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia, 2023), which integrates SPMI with the national accreditation system and expands its scope. SPMI requires universities to implement a continuous quality assurance cycle known as PPEPP (Penetapan, Pelaksanaan, Evaluasi, Pengendalian, dan Peningkatan), which ensures that institutional processes, both academic and non-academic, are systematically planned, executed, evaluated, controlled, and improved.

At SGU, however, the implementation of SPMI has historically focused on academic areas, such as curriculum, teaching, and research. This has inadvertently created a governance gap for non-academic records related to human resources, finance, and institutional contracts. These critical documents are often managed in a fragmented manner, lacking the standardized metadata and centralized repositories required for efficient operations and robust compliance.

To provide a practical context for the following literature review, the operational environment at SGU—including its people, processes, and technology—directly informs the selection of theoretical frameworks and technologies to be reviewed in this chapter. This approach ensures that the literature review is a targeted investigation

aimed at solving specific, real-world challenges at the university, rather than a generic summary.

The SGU environment is characterized by three key factors:

- **Technology: A Google-native ecosystem.** The university has fully adopted **Google Workspace for Education Plus (GWS-E+)** as its core platform for collaboration and daily operations. This technological infrastructure is both a constraint and an opportunity. It justifies a deep focus on solutions native to this ecosystem, such as Google's AI services (Vision, Vertex, and Gemini), as well as low-code platforms like AppSheet. This approach avoids the significant costs and integration complexities associated with reviewing external platforms.
- **Processes: Manual and fragmented governance.** As discussed in Chapter 1, the university's non-academic document management processes are largely manual, inconsistent, and decentralized. This context necessitates a review of robust, structured **governance frameworks**. Therefore, the literature review will prioritize internationally recognized standards that can bring order to this environment: TOGAF for the architectural process, ISO 15489/23081 for records management rules, and COBIT for IT governance and control.
- **People: A Diverse User Base.** The administrative staff at SGU has a wide range of digital skills. While they are familiar with basic Google Workspace tools, they are not technical experts. This human factor makes usability and user adoption critical for the success of any new system. Therefore, the literature review will incorporate principles of **user-centred design** and prioritize evaluation methods that directly measure the user experience, such as the System Usability Scale (SUS).

The context of this study is a technologically equipped yet process-challenged organization with a diverse user base. This context provides the lens through which the following literature is reviewed. Each discussed framework and technology have been selected for its direct relevance to solving problems in this unique environment.

2.3 Theoretical Foundations of Document and Knowledge Governance

Effectively managing organizational information assets is essential for ensuring operational efficiency, supporting informed decision-making, and maintaining a competitive advantage. This section critically examines the fundamental concepts and prevailing theories of document and knowledge management, as well as the challenges that persist in these fields. The section emphasizes their interconnectedness and importance in establishing a robust governance system.

2.3.1 Core Concepts and Interplay

Effective management of an organization's intellectual assets is critical to sustaining operational efficiency, ensuring regulatory compliance, and maintaining a competitive advantage. This requires an understanding of **Document Management (DM)**, **Knowledge Management (KM)**, and **Information Governance (IG)**. Together, these fields establish the structures and processes necessary for the systematic control, accessibility, and accountability of institutional information.

Document management (DM) is defined as the systematic control of documents throughout their lifecycle. This includes everything from creation and capture to storage, distribution, usage, and eventual archiving or disposal (*ISO 15489-1:2016*, 2021). The primary objective of DM is to ensure the Authenticity, Reliability, Integrity, and Usability (ARIU principles) of organizational records. This serves as verifiable evidence of business activities, decisions, and transactions. DM provides the structured processes and systems necessary to organize and maintain explicit information, ensuring that it is discoverable, accessible, and trustworthy.

Knowledge management (KM) is a broad, multidisciplinary field that focuses on the processes by which organizations create, acquire, share, use, and manage explicit and tacit knowledge in order to improve performance and encourage innovation (Davenport and Prusak, 1998). Despite its distinct nature, KM is intrinsically connected to other fields. Explicit knowledge is often codified and formalized. It includes data, information, and documented procedures, which makes it readily transferable. In

contrast, tacit knowledge is highly personal and experience-based. It is difficult to articulate or formalize and resides in individuals' minds.

The relationship between document management (DM) and knowledge management (KM) is symbiotic and hierarchical. Robust document management practices are foundational to effective knowledge management. Documents are the primary means of conveying explicit knowledge. Systematic document capture, organization, and preservation through DM practices facilitate the conversion of tacit knowledge into explicit forms (e.g., documented processes, reports, or best practices) and enable the efficient combination of existing explicit knowledge to generate new insights (Seghroucheni, Achhab and Lazaar, 2023). Without effective DM, however, explicit knowledge can become fragmented, inaccessible, or unreliable, thereby impeding organizational learning, decision-making, and innovation.

Information Governance (IG) is an overarching framework that provides strategic direction and accountability for all information assets, regardless of their format or location. IG ensures information is managed effectively, ethically, and in compliance with regulations throughout its entire lifecycle. It aligns information management with organizational strategy (Steuperaert, 2019). It establishes the policies, processes, and controls necessary to optimize the value of information while mitigating risks. In this context, both DM and KM operate under the umbrella of IG, ensuring that the creation, use, and preservation of documents and knowledge contribute to the organization's strategic goals and compliance obligations.

2.3.2 Challenges in DM & KM

Despite the recognized strategic importance of effective document management (DM) and knowledge management (KM), organizations universally encounter significant challenges in efficiently and compliantly managing their information assets. These challenges are particularly evident in large, complex institutions, such as universities, where the volume and diversity of information, coupled with strict regulatory requirements, present major obstacles. Some common and persistent challenges include:

- **Information Silos and Fragmentation:** A widespread issue that arises when data and documents are dispersed across various departmental systems, individual network drives, personal cloud accounts, or even email inboxes. This results in isolated repositories and a significant absence of a unified, comprehensive view of organizational information (Maltese, 2018; Nguyen Thi Kim, Nguyen Hoang and Nguyen, 2025). This fragmentation directly contributes to *"knowledge fragmentation,"* making it arduous to locate, share, and leverage critical institutional knowledge. This challenge has been identified as a key issue within SGU's non-academic departments, as outlined in Chapter 1.
- **Lack of Version Control:** Inconsistent or absent mechanisms for managing document versions create significant confusion and operational risks. Without clear versioning, users may unknowingly access or work with outdated information, leading to errors in decision-making, duplicated efforts, and a lack of accountability for content changes (Maltese, 2018; Helmholtz Metadata Collaboration (HMC) and Buttigieg, 2022). The absence of a systematic approach to versioning undermines the reliability and integrity of digital records.
- **Inconsistent Metadata and Taxonomy:** The lack of standardized classification schemes, controlled vocabularies, and consistent metadata application across an organization significantly impedes information retrieval efficiency. Without proper tagging and categorization, finding relevant documents becomes arduous, time-consuming, and often reliant on individual memory rather than systematic search (Maltese, 2018). This issue directly contributes to the *"inconsistent metadata"* problem observed at SGU, making it difficult to effectively organize and discover documents.
- **Absence of a "Single Source of Truth":** The combined impact of fragmented storage, ineffective version control, and inconsistent metadata is the inability to confidently assert a definitive, authoritative, and reliable version of organizational information (Maltese, 2018). The absence of a *"single source of truth"* hinders the accuracy of reporting, complicates compliance audits, and undermines strategic planning, as decision-makers may rely on incomplete or contradictory information.
- **Operational Inefficiencies:** Manual, paper-based, or poorly digitized processes often result in significant operational inefficiencies. This includes duplicated

efforts, excessive time wasted searching for information, and bottlenecks in workflows. All of these factors substantially reduce productivity and increase operational costs (R. Choudhary *et al.*, 2024). These inefficiencies can be particularly detrimental in administrative functions that handle high volumes of documents, such as human resources and finance.

These challenges are consistently corroborated by empirical studies. Research on the implementation of knowledge management in Indonesian higher education often emphasizes the *"very diverse and unstructured"* practices common to universities. This indicates a systemic lack of standardized document management frameworks (Hidayat and Sensuse, 2022). These findings align precisely with the operational and information governance deficiencies identified within SGU through preliminary observations and stakeholder input (see Chapter 1, Ishikawa diagram). The persistence and widespread nature of these challenges underscore the critical need for comprehensive, integrated, technologically advanced solutions to improve document and knowledge governance.

Addressing these foundational challenges requires a robust, principled framework. Although an organization could develop its own set of rules, it would lack the rigor, global recognition, and interoperability of an established international standard. Thus, this research adopts **ISO 15489-1:2016** (*"Information and documentation — Records management"*) as its foundational standard.

2.3.3 ISO 15489: International Standard for Records Management

The ISO 15489-1:2016 standard, titled *"Information and documentation — Records management — Part 1: Concepts and Principles"* serves as a foundational international benchmark for effective records management practices. It provides a robust framework outlining the principles and processes necessary to manage records throughout their lifecycle, ensuring their authenticity, reliability, integrity, and usability (ISO 15489-1:2016, 2021). Adherence to ISO 15489 is not merely a matter of compliance but is crucial for:

- **Establishing Accountability and Transparency:** Records serve as vital documentation of business activities and decisions, ensuring organizational accountability.

- **Mitigating Legal and Regulatory Risk:** Proper records management ensures compliance with legal obligations, industry regulations, and internal policies, thereby reducing the risk of litigation or penalties.
- **Supporting Business Processes:** A well-managed records system facilitates efficient operations by ensuring that necessary information is readily available when and where it is needed.
- **Preserving Institutional Memory:** Records serve as the collective memory of an organization, playing a critical role in learning, continuity, and historical preservation.

2.3.3.1 Justification for Adopting ISO 15489

The selection of ISO 15489 was a deliberate architectural decision based on three key factors:

- ***Direct Problem Alignment:*** ISO 15489 provides direct, authoritative answers to core challenges. Its principles for ensuring the authenticity, reliability, integrity, and usability (ARIU) of records are specifically designed to combat information fragmentation and establish a reliable *"single source of truth."*
- ***Global Best Practice:*** As the international benchmark for records management, adopting it ensures that the proposed system is built on globally recognized best practices. For an international institution like SGU, this provides a level of credibility and a future-proof foundation that proprietary or custom solutions cannot.
- ***Strategic Complement to SPMI:*** As noted in the case study, SGU's SPMI framework focuses on academic quality. ISO 15489 supplements SPMI strategically by providing governance principles for the non-academic domain, creating a more holistic institutional quality assurance ecosystem.

2.3.3.2 Application of ISO 15489 Principles in This Research

Full organizational certification to ISO 15489 is outside the scope of this PoC. Instead, this research will embed the standard's core principles directly into the system's architecture and functionality. The specific *"jobs"* of the standard in this project are to:

- **Guide Lifecycle Management:** The system's design addresses the fragmented practices at SGU by managing digital documents from creation and capture to use and disposition.
- **Enforce metadata standards:** The standard requires robust and consistent metadata. The system's automated tagging and classification features will operationalize this principle, aligning with ISO 23081 (as discussed in Section 2.3).
- **Define Classification and Organization:** ISO 15489 principles will inform the development of a logical taxonomy for SGU's non-academic documents. This taxonomy is essential for reducing information silos and improving discoverability.
- **Implement Access and Security Controls:** The design will incorporate role-based access controls to ensure that records are secure and access is managed appropriately, which is a key requirement of the standard.

2.4 Metadata Governance and Contract Deadline Control

Effective document governance depends on more than just where documents are stored; it also depends on how well they are described, classified, and made retrievable through the use of metadata. Metadata, often defined as "*data about data*," plays a central role in ensuring that digital records are searchable, traceable, understandable in context, and legally defensible over time. Inadequate or inconsistent metadata is widely cited in literature as a key barrier to findability, access control, lifecycle management, and legal defensibility (Hughes *et al.*, 2023).

In higher education institutions, metadata issues often arise from siloed departmental structures, inconsistent tagging practices, and unclear ownership of metadata. These issues result in fragmented document ecosystems, inefficient searches, and an inability to enforce records policies—problems evident in SGU's current operational context. One significant consequence of this fragmentation is the inability to effectively monitor contract deadlines, which has historically resulted in renewal delays and policy breaches. This research addresses these issues directly by designing an AI-enhanced

document governance system that embeds standardized metadata fields, including critical contract expiration dates, to enable automated tracking and notifications.

2.4.1 Theoretical Foundations of Data Governance and Metadata Management

Effective data governance and robust metadata management are essential for ensuring the quality, consistency, and usability of an organization's information assets (Aprilia Eka Putri and Muhammad Irwan Padli Nasution, 2025). These areas emphasize several fundamental principles that are critical to designing and operating any intelligent document governance system.

- ***Standardized Vocabulary and Classification:*** According to Nakash (2024), consistency in document tagging, achieved through the use of controlled vocabularies, taxonomies, and hierarchical classification schemes, is essential for enabling accurate indexing, filtering, and semantic retrieval. This is especially important for diverse document types, particularly contract documents, where inconsistent naming of entities (e.g., vendors, document types, or expiration terms) can severely hinder automated notifications and compliance workflows (Nakash, 2024).
- ***Data Quality Dimensions:*** The widely recognized data quality dimensions—accuracy, consistency, completeness, timeliness, validity, and uniqueness—should guide the design and evaluation of any metadata system (Kumar, Chandrappa and Harinarayana, 2024). These dimensions are especially important in document systems where metadata directly affects searchability, auditability, and compliance reporting. For SGU, timeliness becomes a critical factor because accurately and current tracking of contract expiration dates directly impacts legal and operational continuity by mitigating the risk of missed renewals.
- ***Metadata Stewardship and Ownership:*** Clearly assigning responsibility for creating, entering, reviewing, and maintaining metadata is essential for the system's long-term sustainability and integrity. This principle is rooted in data stewardship theory, which emphasizes accountability and the ongoing governance of information assets (Plotkin, 2013).

Relevance to this research: Although ISO 15489 establishes high-level principles for records management, effective governance is impossible without consistent, structured metadata. The literature confirms that consistent, structured metadata is essential for avoiding poor information retrieval and operational risk. To operationalize ISO 15489, this research formally adopts **ISO 23081-1:2017** ("*Information and documentation — Managing metadata for records*") as the guiding standard for the system's metadata architecture. By embedding the principles of this standard into the system, the study aims to eliminate metadata inconsistencies and increase institutional control. The proposed system will ensure that documents are consistently tagged and linked to automated reminders for critical deadlines, such as contract expiration dates. This will reduce administrative risk and ensure that records remain reliable, accessible, and trustworthy.

2.4.2 ISO 23081: International Standard for Metadata for Records

In addition to theoretical frameworks, this research is informed by internationally recognized standards for records and metadata management, particularly ISO 23081. ISO 23081 provides a structured approach to defining and managing metadata, supporting the authenticity, reliability, and usability of records throughout their lifecycle. Together with ISO 15489, which establishes core principles for records management, ISO 23081 ensures the proposed system effectively manages documents and enforces consistent metadata governance. This enables reliable retrieval, policy compliance, and long-term institutional accountability.

ISO 23081-1:2017, "*Information and documentation — Managing metadata for records — Part 1: Principles*," (ISO 23081-1:2017, 2023) outlines best practices for metadata in records systems. The standard defines metadata as structured or semi-structured information that enables the identification and classification of records:

- Identification and classification of records: Ensuring documents are correctly categorized for easy retrieval.
- Management of access rights: Facilitating granular control over who can access specific information.
- Retention scheduling: Supporting automated or semi-automated management of document lifecycles.

- **Audit trail creation:** Providing verifiable evidence of actions performed on records for accountability and transparency.

2.4.2.1 Justification for Adopting ISO 23081

The selection of ISO 23081 is a necessary and logical extension of the commitment to ISO 15489 for two main reasons:

- ***Direct and Seamless Integration:*** ISO 23081 is not a competing standard, but rather a complementary one designed to work directly with ISO 15489. It provides specific instructions for the metadata principles that ISO 15489 requires. Selecting a different metadata framework could create conflicts and diminish the coherence of the overall governance architecture.
- ***Enabler for AI Automation:*** The standard's structured approach is essential for the AI components of the system. AI tools such as the Google Vision API and Gemini require consistent and predictable metadata schemas in order to accurately classify documents and extract key information (e.g., contract expiration dates). ISO 23081 provides the formal structure needed to "teach" the AI what to look for, transforming the system from a passive repository into a proactive compliance tool.

2.4.2.2 Application of ISO 23081 in This Research

This study developed a system that embeds ISO-compliant metadata fields into the core design of all key document types. The specific roles of the standard in this project are to:

- ***Define the metadata scheme:*** The standard provides guidance on defining essential metadata fields for contracts, policies, and HR forms to ensure that data quality dimensions such as accuracy, completeness, and timeliness are met.
- ***Automate information extraction:*** AI tools are configured to automatically identify and populate these predefined metadata fields, reducing manual entry and ensuring consistency.

- **Enable proactive monitoring:** Lifecycle metadata fields, such as creation and expiration dates, are linked to automated alerts via Google Calendar, which is central to the project's contract monitoring function.
- **Support audit and compliance:** Structured metadata creates a reliable audit trail that provides verifiable evidence of actions performed on records. This is essential for accountability and transparency.

Integrating these two ISO standards creates a comprehensive governance framework. ISO 15489 establishes the general rules for records management, and ISO 23081 provides the specific data structure necessary to effectively enforce those rules. The table below summarizes their distinct yet complementary contributions.

Table 2.1 Summary of Selected Records and Metadata Governance Standards

Standard	Primary Focus	Specific Aspects Utilized in This Research
ISO 15489: Records Management	Principles and requirements for managing records throughout their lifecycle	Provides internationally recognized best practices for trustworthiness, accessibility, and lifecycle control; informs system design for capture, classification, and secure storage.
ISO 23081: Metadata for Records	Framework for creating, managing, and maintaining metadata in records systems	Defines metadata elements essential for record authenticity, reliability, and integrity; supports structured search, automated classification, and AI-driven contract monitoring features.

2.5 Enterprise Architecture (EA) and IT Governance Frameworks

Aligning information technology (IT) with business strategy is critical for modern organizations, especially in complex institutional environments like universities. Aligning IT with business strategy ensures that IT investments support day-to-day operations and advance long-term institutional objectives. Enterprise architecture (EA) and IT governance frameworks play a strategic role in this process by providing structured methodologies and principles that maximize business value, manage risks effectively, and ensure regulatory compliance. This section critically reviews key EA and IT governance frameworks, emphasizing their strategic importance and explaining why they were chosen as the foundation of the proposed intelligent document governance system for SGU.

2.5.1 Enterprise Architecture (EA) Principles and Purpose

Enterprise architecture is a comprehensive practice that describes and analyzes all elements of an enterprise, including its business processes, information flow, applications, and technology infrastructure. Its primary purpose is to provide a comprehensive plan that guides organizational change and ensures that IT initiatives are strategically aligned with business objectives. EA bridges the gap between business strategy and IT implementation, enabling organizations to optimize their operations, enhance agility, and manage complexity (Abunadi, 2019).

EA frameworks generally define various architectural domains (Kotusev, 2017), such as:

- **Business Architecture:** This document meticulously articulates the organization's strategic direction, governance framework, organizational structure, and pivotal business processes.
- **Data Architecture:** This document provides a comprehensive overview of the organization's data assets, both logical and physical, along with an analysis of its data management resources.
- **Application Architecture:** It provides a blueprint for individual application systems and their interactions.
- **Technology Architecture:** This text delineates the logical software and hardware requirement that are necessary to support the deployment of business, data, and application services.

The advantages of a well-defined EA are widely recognized, including improved decision-making, reduced IT costs, enhanced responsiveness to change, and better risk management. However, successful EA implementation is contingent upon clear methodologies, strong leadership, and continuous adaptation to evolving organizational needs. Challenges often arise from its inherent complexity, the significant resources required for its establishment and maintenance, and the potential for it to become a purely academic exercise if not directly tied to business value (Kotusev, 2017). For higher education institutions, EA can provide the necessary structure to integrate

disparate campus systems and processes, promoting efficiency and supporting strategic goals like digital transformation (Adepoju *et al.*, 2024).

2.5.2 Overview of Prominent Enterprise Architecture Frameworks

There are several EA frameworks in existence, each with distinct strengths and areas of focus. It is crucial to understand these differences when selecting the most appropriate framework for a given context.

2.5.2.1 The Zachman Framework for Enterprise Architecture

Introduced by John Zachman in 1987, the Zachman Framework is recognized as one of the earliest and most influential contributions to enterprise architecture (EA). It is presented as a 6×6 matrix where the columns represent six fundamental questions ("*What*," "*How*," "*Where*," "*Who*," "*When*," and "*Why*") and the rows capture six stakeholder perspectives, ranging from strategic planners to system users. Each cell corresponds to a descriptive artifact, offering a holistic view of the enterprise collectively (Kotusev, 2021).

The framework offers value by standardizing EA documentation, facilitating communication across organizational levels, and helping identify coverage gaps. In practice, it is often used alongside process-oriented frameworks, such as The Open Group Architecture Framework (TOGAF), where Zachman provides the structural reference and the other framework offers methodological guidance. However, organizations that attempt to apply the framework literally by producing exhaustive documentation have often incurred high costs and limited practical benefits (*A comparison of the top four enterprise architecture frameworks* | BCS, 2021).

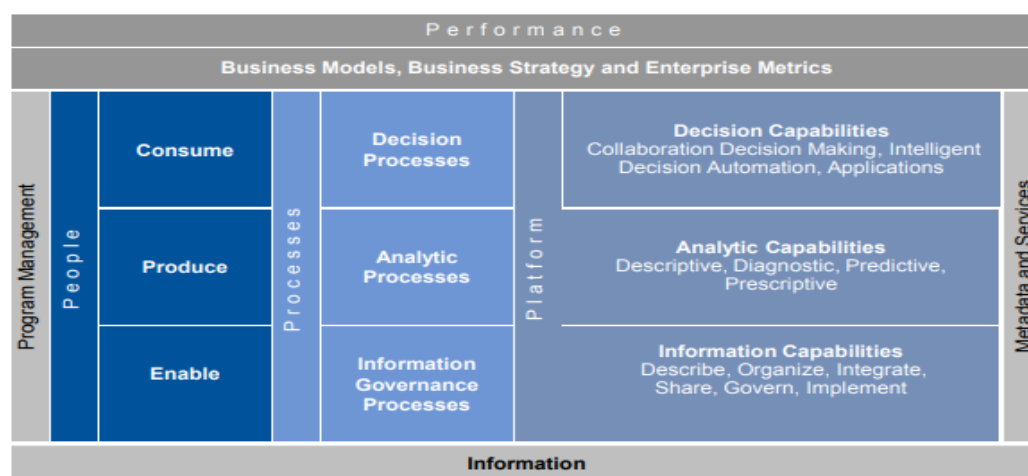
Overall, the Zachman Framework is best understood as a taxonomy rather than a methodology. It provides a classification structure to organize architectural artifacts, but it does not prescribe how to develop or implement enterprise architecture. This limits its applicability as a standalone framework for research or projects requiring reproducibility, compliance mapping, or methodological rigor.

2.5.2.2 Gartner Enterprise Architecture

The Gartner Enterprise Architecture (EA) approach views EA as an ongoing management discipline rather than a one-time project. It ensures alignment between business strategy and IT requirement while delivering measurable business value. Rather than prescribing specific phases or artifacts, the approach provides guiding principles that can be adapted to an organization's level of maturity and unique requirements (Chandler *et al.*, 2012). Figure 2.1 illustrates the Gartner EA approach as a business-driven, adaptive practice.

A distinctive strength of the Gartner approach is its emphasis on business outcome orientation, stakeholder engagement, and continuous alignment. Business and IT leaders consistently collaborate to ensure that IT investments remain aligned with changing organizational priorities. This flexibility enables institutions to respond to evolving demands and avoids the inflexibility often associated with methodology-heavy frameworks (Chandler *et al.*, 2012).

However, Gartner's approach has limitations. It lacks a prescriptive methodology, standardized artifacts, and a modelling language, which can pose challenges for organizations seeking structured documentation or compliance-oriented frameworks. Additionally, its reliance on proprietary Gartner research and advisory services may create accessibility and cost barriers (Chandler *et al.*, 2012). Thus, while Gartner is highly effective at guiding enterprise architecture (EA) at a strategic level, it is often best used in combination with more structured frameworks when detailed architectural development is required.



Source: Gartner (September 2011)

Figure 2.1 Gartner Framework
Source: (Chandler et al., 2012)

2.5.2.3 Federal Enterprise Architecture Framework (FEAF)

The U.S. government developed FEAF to provide a common language and approach for IT modernization within federal agencies. It emphasizes business-driven EA development and incorporates various reference models (e.g., Performance Reference Model, Business Reference Model) (Rouhani *et al.*, 2015). FEAF's primary strength lies in its emphasis on government, performance, and business outcomes, offering valuable reference models that align IT initiatives directly with public sector objectives through its six interconnected reference models linked through the Consolidated Reference Model (CRM).

However, its primary limitation is its highly tailored nature to the U.S. federal context. This makes it less universally applicable without significant adaptation for other sectors or countries, which limits its direct utility for a university in Indonesia (Kotusev, 2021). In addition, the FEAF implementation process has encountered notable challenges. Critics have asserted that a considerable portion of FEAF expenditure has led to wasteful spending, and contemporary experts have raised questions regarding its practical value to modern practitioners (Rouhani *et al.*, 2015). The framework's emphasis on federal government operations and compliance requirements makes it ill-suited for direct application in different organizational contexts without extensive modification.

2.5.2.4 The Open Group Architecture Framework (TOGAF)

TOGAF, developed and maintained by The Open Group, is one of the most widely adopted and comprehensive EA frameworks globally. Its strength lies in providing a robust, iterative process for developing and managing enterprise architectures, known as the Architecture Development Method (ADM) (Kotusev, 2018). Like shown in figure 2.2, the ADM methodically guides architects through the various stages of the process, from the initial conception to the implementation phase, ensuring a systematic approach to aligning business objectives with information technology (*TOGAF* | www.opengroup.org, 2025). TOGAF also offers an extensive Architecture Content Framework and Reference Models, facilitating consistency and accelerating development.

From a business perspective, TOGAF's comprehensive approach is a significant strength. Its ADM covers the entire lifecycle of architecture development, from strategic planning to implementation and ongoing governance, offering a holistic view (Ulmi *et al.*, 2020). This adaptability and customizability are crucial for organizations with unique operational nuances, such as SGU. It allows for tailoring to specific organizational contexts, rather than rigid adherence to a standard. Its widespread industry adoption across various sectors further validates its practical utility and the robustness of its principles. Its structured, iterative ADM promotes continuous improvement and allows for beneficial feedback loops in complex digital transformation projects.

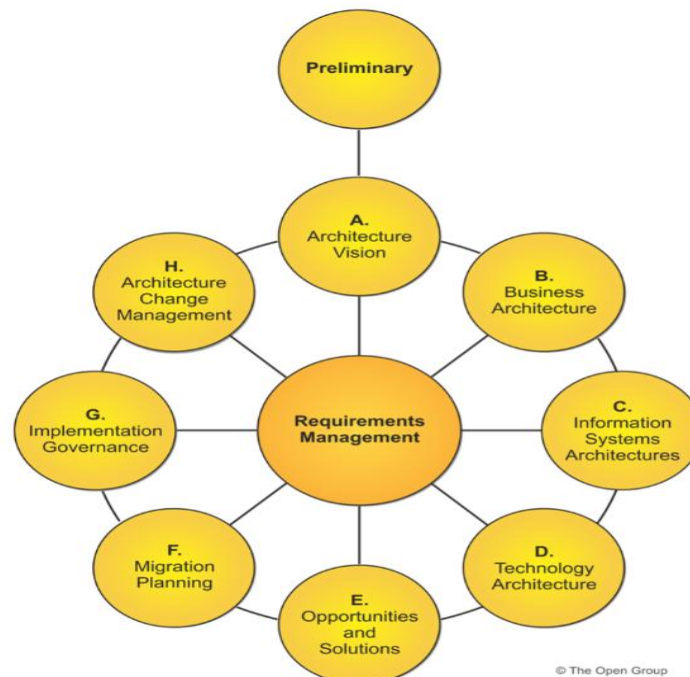


Figure 2.2 TOGAF Framework
Source: (Open Group, 2025)

However, TOGAF has been the subject of criticism regarding its complexity and resource intensity. It has been described as overly prescriptive, requiring significant resources, time, and specialized expertise for effective implementation (Kotusev, 2018). Through empirical case study analysis, Kotusev (2018) found that TOGAF's inherent complexity requires substantial organizational adaptation, with none of the TOGAF-specific recommendations proving useful in actual practice. This finding calls into question the framework's value as a standard for enterprise architecture. This inherent complexity can be a deterrent for smaller organizations or those with limited IT budgets. Additionally, enterprise architecture management faces significant implementation challenges due to the complexity of modern information systems architectures. In these architectures, changes to individual components may have unintended effects on multiple related systems (Beese *et al.*, 2023). If strong leadership and clear business alignment are not in place, there is a risk that implementing TOGAF will become an abstract, documentation-heavy exercise that is detached from tangible business value.

2.5.2.5 Justification for Selection of TOGAF as Primary EA Framework

Although there are several Enterprise Architecture (EA) frameworks, TOGAF was chosen for its comprehensive and adaptable Architecture Development Method (ADM). The ADM provides a systematic, step-by-step design process. A comparative analysis confirms its suitability for this specific research context over other prominent frameworks.

Alternative Frameworks Considered:

- The Zachman Framework is a powerful tool for classifying architectural artifacts, but it is a taxonomy, not a methodology. It provides no procedural guidance for designing or implementing a system.
- The Federal Enterprise Architecture Framework (FEAF) is highly specialized for the U.S. federal government, rendering its reference models and processes unsuitable for the Indonesian higher education context.
- The Gartner EA Approach offers valuable strategic insights focused on business outcomes, but it lacks a prescriptive, repeatable methodology and standardized artifacts. These are essential for the academic rigor of a proof of concept (PoC).

TOGAF's ADM provides the ideal balance, offering a structured yet flexible roadmap lacking in the other frameworks. It ensures that the system design is coherent, complete, and directly aligned with SGU's institutional goals.

2.5.2.6 Application of TOGAF in This Research

A full, enterprise-wide implementation of TOGAF is beyond the scope of this proof of concept (PoC). Instead, this research project will apply the principles of the TOGAF ADM strategically to guide the system's design. TOGAF's specific role in this project is to:

- ***Provide a structured design process:*** Key phases of the ADM—specifically Phases B (Business Architecture), C (Information Systems Architectures), and D (Technology Architecture)—will be used to structure the design of the artifact, ensuring a holistic approach.

This selective application of the ADM provides the necessary architectural rigor for the PoC while remaining within the project's practical scope. The following table summarizes the comparative analysis.

Table 2.2 Comparison of Prominent Enterprise Architecture Frameworks

Framework	Strengths	Limitations	Contextual Fit for This Study
TOGAF (The Open Group Architecture Framework)	Comprehensive, structured methodology (ADM); iterative and adaptable.	Can be complex and resource-intensive for full implementation.	Selected as primary framework; ADM Phases B–D guide PoC design; adaptable to SGU’s needs.
Zachman Framework	Provides structured taxonomy; ensures comprehensive classification.	Not a methodology; lacks procedural guidance for implementation.	Useful for classifying artefacts, but not suitable for guiding PoC design.
FEAF (Federal Enterprise Architecture Framework)	Strong focus on public sector outcomes; standardized reference models.	Tailored to U.S. federal context; limited global applicability.	Rejected due to contextual mismatch with Indonesian higher education.
Gartner EA Approach	Emphasizes business outcomes and stakeholder engagement.	Lacks prescriptive methodology and standardized artifacts.	Valuable for strategic insight but insufficient rigor for PoC design.

2.5.3 Overview of Prominent IT Governance Frameworks

Information technology (IT) frameworks are structured sets of best practices, principles, and governance models that guide organizations in managing IT services, infrastructure, and resources in alignment with strategic business goals. IT frameworks enhance efficiency, ensure accountability, minimize risk, and improve service quality in IT operations (Mr. N. Suresh, Dr T. Varalakshmi, and Mohd Shoaib Chand, 2024).

Unlike enterprise architecture frameworks, such as The Open Group Architecture Framework (TOGAF), which focus on high-level planning, design, and transformation of the enterprise, IT frameworks provide operational and tactical guidance. IT frameworks standardize the delivery of IT services, facilitate compliance with regulatory requirements, and support the implementation of internal control mechanisms, such as role-based access, audit trails, and service monitoring (*COBIT | Control Objectives for Information Technologies*, 2019).

In the context of this study, IT frameworks play a pivotal role in embedding governance and operational discipline into the design and evaluation of the intelligent document and contract management system. Integrating IT frameworks ensures the proposed system fulfills functional and nonfunctional requirements, adheres to institutional policies, supports accountability, and aligns with international standards for security, service management, and metadata governance.

2.5.3.1 ITIL 4 (Information Technology Infrastructure Library):

The Information Technology Infrastructure Library (ITIL) is one of the most widely adopted frameworks for IT Service Management (ITSM). It is designed to align IT services with business needs. Originally developed by the UK government's Central Computer and Telecommunications Agency (CCTA), ITIL has evolved over several decades and is currently managed by AXELOS. The most recent version, ITIL 4, was released in 2019. It represents a significant shift from previous versions by incorporating principles from Agile, DevOps, and Lean. This ensures flexibility and responsiveness in modern digital environments (LIMITED, 2019).

ITIL 4 introduces a Service Value System (SVS) and a set of guiding principles that emphasize the co-creation of value through service relationships. In figure 2.3 below, the SVS includes five key components: guiding principles, governance, the service value chain, practices, and continual improvement (*A Beginner's Guide to ITIL 4 Principles* | Atomicwork, 2019). This holistic approach helps organizations manage the full lifecycle of IT services—from strategy and design to operation and continual service improvement—while fostering agility and resilience in the face of digital transformation.

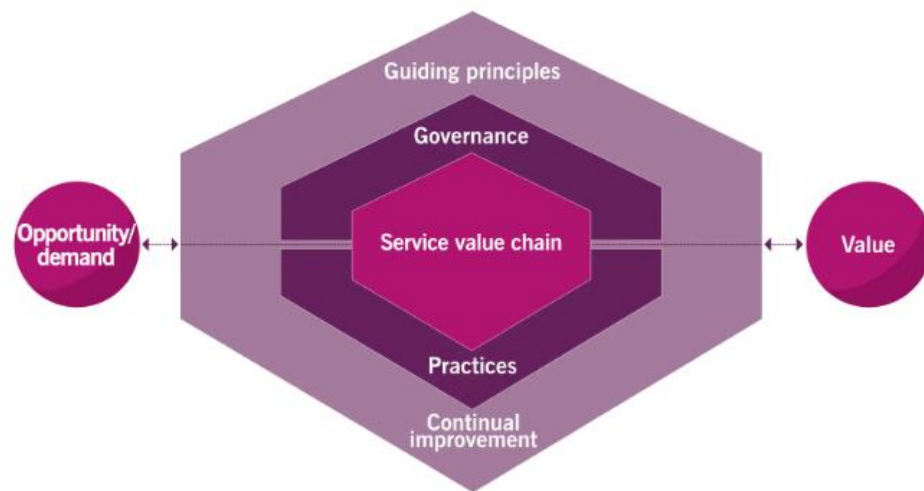


Figure 2.3 ITIL4 Service Value System
Source: (ManageEngine, 2024)

ITIL 4's primary strengths lie in its operational effectiveness and detailed practices for delivering and supporting high-quality IT services. Key practices include incident management, problem management, change control, service desk operations, and service level management (TheKnowledgeAcademy, 2025). These practices are essential for ensuring service continuity, responsiveness, and user satisfaction, particularly in large, complex IT environments.

Despite its strengths in managing operational IT services, ITIL 4 provides limited guidance for the design and development of new IT systems. Its primary focus lies in service delivery and support processes, rather than in system architecture, strategic planning, or governance structures. As such, it lacks the comprehensive frameworks needed to guide the early stages of system development, such as requirement alignment, risk-based decision-making, and enterprise-wide integration (TheKnowledgeAcademy, 2025).

2.5.3.2 ISO/IEC 27001 (Information Security Management Systems)

ISO/IEC 27001 is an internationally recognized standard that outlines the requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). The standard takes a risk-based

approach to safeguarding information assets and ensuring their confidentiality, integrity, and availability (Kitsios, Chatzidimitriou and Kamariotou, 2023). Applicable to organizations of all sizes and sectors, ISO/IEC 27001 provides a systematic methodology for identifying, assessing, and mitigating security risks through clearly defined policies, procedures, and controls (Culot *et al.*, 2021).

A key strength of ISO/IEC 27001 is its specialized focus on information security. It provides a robust framework for risk assessment and treatment supported by ISO/IEC 27002, which details security controls and implementation guidance. Certification formally recognizes an organization's commitment to information security best practices, strengthening regulatory compliance, stakeholder trust, and competitive positioning in security-sensitive sectors (Culot *et al.*, 2021).

However, its scope is intentionally narrow, focusing solely on information security rather than on broader IT governance, value delivery, or enterprise architecture. While indispensable for securing digital assets, ISO/IEC 27001 does not address strategic alignment, resource optimization, or performance monitoring, which are found in more comprehensive governance frameworks, such as COBIT 2019 and ITIL 4.

Its generic, cross-industry requirements demand significant contextual adaptation for effective implementation. Furthermore, literature notes that adoption is often driven by external pressures, such as regulatory mandates and market differentiation, rather than as part of an integrated governance strategy (Kitsios, Chatzidimitriou and Kamariotou, 2023). Consequently, while ISO/IEC 27001 is a critical pillar of IT governance, comprehensive coverage often requires integrating it with complementary frameworks.

2.5.3.3 COBIT 2019 (Control Objectives for Information and Related Technologies)

Developed by ISACA, COBIT 2019 is a globally recognized framework for the governance and management of enterprise IT. Designed to help organizations optimize the value of IT, COBIT 2019 balances benefits realization, risk optimization, and

resource optimization (*COBIT | Control Objectives for Information Technologies*, 2019). COBIT 2019 provides a comprehensive set of principles, objectives, and governance system components that align IT initiatives with business objectives. The framework places a strong emphasis on governance, risk, and compliance (GRC) (Abdulrasool and Turnbull, 2020). As illustrated in Figure 2.4, COBIT 2019 is built upon two interrelated sets of principles: Governance System principles, which define how governance should operate within the enterprise, and Governance Framework principles, which describe the framework's characteristics. Together, these principles ensure that COBIT remains conceptually rigorous while being adaptable to diverse organizational contexts.

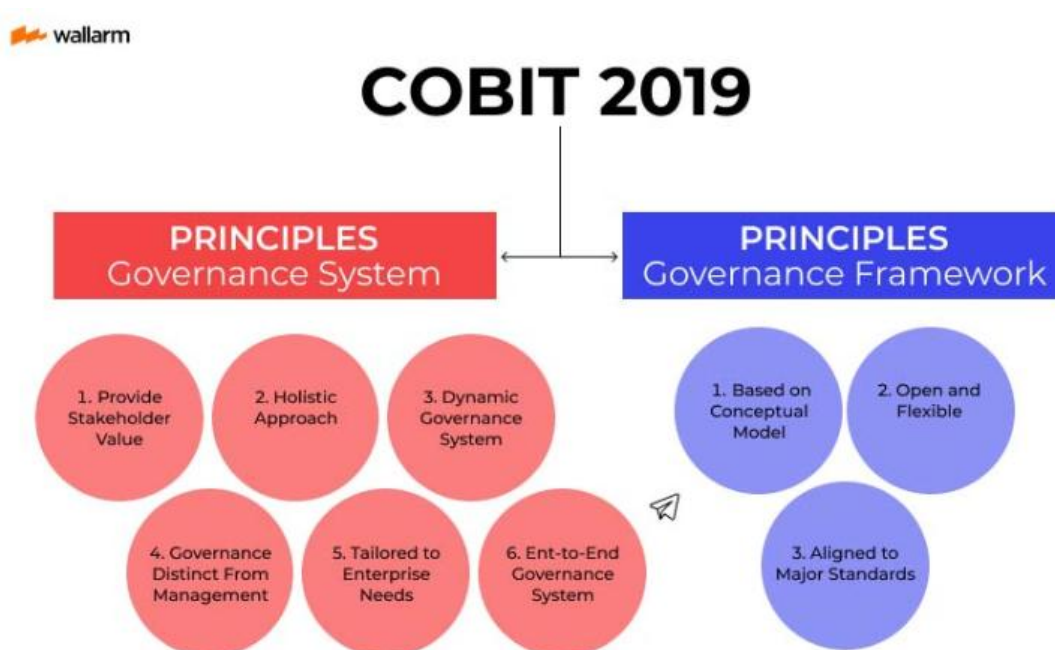


Figure 2.4 COBIT 2019 Principles
Source: (Ivan Lee, 2025)

From a critical standpoint, COBIT's most significant strength lies in its holistic governance focus, which effectively links IT processes directly to broader business objectives and value creation across the enterprise. It is particularly robust in its risk and compliance orientation, offering detailed guidance for identifying, assessing, and managing IT-related risks and ensuring adherence to regulatory requirements (Abdulrasool and Turnbull, 2020). This aspect is highly relevant given SGU's internal

quality assurance (SPMI) and general compliance needs for sensitive documents. Furthermore, COBIT's incorporation of maturity models enables organizations to methodically evaluate their current IT process landscape and pinpoint specific areas for enhancement, thereby cultivating a culture of continuous improvement through requirement and maturity level assessments ranging from Level 0 (incomplete) to Level 5 (optimizing) (Hidayat, Indrajit and Dazki, 2024).

However, COBIT can be perceived as complex and resource-intensive for organizations, particularly smaller ones or those with limited IT maturity. Implementing the full scope may require significant effort and expertise, as studies indicate that many organizations face challenges in achieving higher maturity levels, often remaining at Level 2 (Managed) with notable gaps between current and desired maturity targets (Hidayat, Indrajit and Dazki, 2024). While it provides a robust framework for control and audit, it is less prescriptive on how to implement specific technological solutions. It serves more as a guiding framework for governance and high-level management rather than a detailed implementation methodology for IT operations.

2.5.3.4 Justification for Selecting COBIT 2019

Although TOGAF provides an architectural blueprint for the system, it does not provide a framework for IT governance on its own. A purely architectural approach may result in a functional system that lacks the necessary controls for risk management, compliance, and strategic alignment with institutional goals. This research addresses this gap by integrating COBIT 2019 as the guiding framework for IT governance.

COBIT 2019 was selected because of its unique position as a holistic governance framework that connects IT processes to business value. A comparative analysis demonstrates why COBIT 2019 is better suited for this research than other common IT frameworks.

Alternative Frameworks Considered:

- ITIL 4 is the industry standard for IT service management. While it is excellent for operational processes, such as incident and change management, it lacks the high-level strategic oversight needed for institutional governance and is too tactical.
- ISO/IEC 27001 is a world-class standard for information security management. However, its scope is intentionally narrow, focusing solely on security controls. It does not address broader governance concerns, such as value delivery, resource optimization, or overall process accountability.

COBIT 2019 was chosen because it provides an integrated system that balances these different needs. COBIT 2019 ensures that the proposed solution is technically sound, strategically aligned, compliant, and risk-aware—essential qualities for long-term institutional adoption.

2.5.3.5 Application of COBIT 2019 in This Research

COBIT 2019 will not be implemented in its entirety. Instead, it will serve as a governance lens to guide the design of policies. COBIT's specific “*jobs*” in this project are to:

- ***Inform control-oriented features:*** The design of features such as role-based access control (RBAC), audit logging, and compliance monitoring is directly influenced by COBIT's control objectives.
- ***Guide Policy and Recommendations:*** The recommendations in Chapter 5 will be explicitly linked to relevant COBIT 2019 objectives, such as EDM01 (Ensure Governance Framework Setting and Maintenance) and APO13 (Manage Security). This ensures that the proof of concept (PoC) can be integrated into SGU's broader governance ecosystem.

Pairing TOGAF's architectural method with COBIT's governance principles ensures that the resulting artifact is well-designed and well-controlled. The following table summarizes the comparative analysis.

Table 2.3 Summarize of IT Frameworks Overview

Framework	Strengths	Limitations	Contextual Fit for This Study
COBIT 2019 (Control Objectives for Information and Related Technologies)	Holistic governance focus linking IT to business value; strong risk and compliance orientation.	Can be complex and resource-intensive for full implementation.	Selected as the complementary governance framework; ensures strategic alignment, risk management, and auditability for the PoC.
ITIL 4 (Information Technology Infrastructure Library)	Industry-standard for IT service management (ITSM); detailed operational best practices.	Lacks strategic governance and enterprise-wide risk focus.	Valuable for operations, but lacks the governance oversight needed for PoC design and institutional risk alignment.
ISO/IEC 27001 (Information Security Management)	Globally recognized security standard; strong in risk-based security controls.	Specialized focus limited to information security; does not address broader IT governance.	Not selected due to narrow scope; broader governance principles are required for PoC sustainability.

2.6 Artificial Intelligence (AI) in Document Governance

The exponential growth of digital information has fundamentally changed how organizations manage documents. This shift requires systems that go beyond storage to ensure efficient retrieval, structured organization, and regulatory compliance (Mahadevkar *et al.*, 2024). Artificial intelligence (AI), which encompasses machine learning (ML), natural language processing (NLP), optical character recognition (OCR), and intelligent document processing (IDP), is increasingly recognized as a transformative enabler in document governance.

This section reviews the conceptual foundations of AI, its practical applications in document governance, the benefits of AI, and the challenges that persist. Then, it justifies the adoption of AI in this research and critically compares alternative tools.

2.6.1 Core AI Concepts for Document Management

The integration of AI in document management systems (DMS) utilizes complementary technologies that transform unstructured and semi-structured content into structured, actionable information:

- **Machine Learning (ML):** Systems can identify patterns and make predictions from large datasets without explicit programming. In document governance, ML supports automated classification, relevance prediction, and adaptive retrieval based on user behavior ((Alyasiri and Cheah, 2025). Continuous learning ensures that the system can adapt to evolving content.
- **Natural Language Processing (NLP):** Allows systems to interpret and generate human language. This requirement supports semantic searches, summarizations, entity recognitions, and contextual analyses that go beyond simple keyword matching (Liu, Yang and Chen, 2025). This requirement is critical for deep document understanding.
- **Optical Character Recognition (OCR):** Converts scanned or image-based text into searchable and editable data. AI-enhanced OCR improves accuracy for complex layouts, varied fonts, and handwriting. This enables search and governance over legacy and paper-based records (Liu, Yang and Chen, 2025).
- **Intelligent document processing (IDP):** It combines OCR, natural language processing (NLP), and machine learning (ML) to capture, extract, and process information from diverse formats. This transforms unstructured content into structured datasets for governance and automation (Haricharan, 2023).

2.6.2 Benefits and Challenges of AI in Document Governance

Integrating AI into document governance provides a variety of tangible benefits that address the operational and strategic needs of modern institutions, such as SGU. First, AI substantially improves **efficiency and speed** by automating labor-intensive tasks, such as classification, data entry, and routing. This reduces the manual workload of administrative staff, allowing them to focus on activities that contribute more directly to institutional goals (Liu, Yang and Chen, 2025).

Equally important are the improvements in **accuracy and consistency**. By minimizing human error in repetitive processes, AI ensures more reliable data extraction and categorization, which is a foundational requirement for effective compliance and governance (Alyasiri and Cheah, 2025).

AI systems also offer inherent **scalability**, making them well-suited to institutions with rapidly growing information repositories. These systems can process document volumes far beyond human capacity while maintaining speed and precision (Mahadevkar *et al.*, 2024).

Furthermore, AI provides deeper insights through **advanced analytics and semantic search requirement**, enabling decision-makers to identify meaningful patterns and context in large collections of unstructured data (Vennila *et al.*, 2024). Finally, AI enhances **compliance and security** by automating policy enforcement, identifying non-compliant content, and creating thorough audit trails. These functions closely align with COBIT's control objectives, ensuring consistent and verifiable application of governance policies (Mahadevkar *et al.*, 2024).

Despite these benefits, several challenges must be addressed to ensure successful adoption. First, AI systems depend heavily on **data quality**; therefore, inaccuracies, inconsistencies, or biases in training data can significantly degrade performance. At SGU, for example, inconsistent metadata standards necessitate rigorous preprocessing to ensure reliable outcomes.

The **complexity and cost of AI implementation** present additional barriers. Deploying effective AI solutions typically requires specialized data science expertise, substantial computational resources, and a significant upfront investment (Mahadevkar *et al.*, 2024). Another critical issue is **explainability**. Many advanced AI models operate as "black boxes," making their decision-making processes difficult to interpret. This opacity can undermine user trust and complicate auditing and regulatory compliance (Mahadevkar *et al.*, 2024).

Finally, **integration and maintenance** are ongoing concerns. It is essential to ensure compatibility with existing legacy systems, maintain robust APIs, and retrain AI models to adapt to evolving document patterns to sustain performance over time (Mahadevkar *et al.*, 2024).

2.6.3 Justification for AI's Inclusion in this Research

The central technical pillar of this research is the inclusion of artificial intelligence (AI), which transforms the proposed system from a simple document repository into an intelligent governance platform. AI-powered features address SGU's core challenges of inconsistent metadata and inefficient information retrieval, as discussed in Chapter 1. Therefore, the decision to use AI is not an addition, but rather the primary mechanism for achieving the study's objectives.

This research leverages SGU's existing Google Workspace for Education Plus (GWS-E+) infrastructure, which provides native access to a suite of powerful AI tools. This approach was chosen to minimize implementation costs, reduce technical complexity, and ensure seamless integration with the tools that SGU staff already use.

2.6.4 Justification and Comparison of AI Tools in the Proposed System

After conducting a comparative analysis of commercial and open-source alternatives, a curated set of tools from the Google Cloud ecosystem was selected to fulfil the system's functional requirements. Although other platforms offer comparable features, they were deemed unsuitable due to higher costs, more complex integration, or security and compliance concerns within SGU's Google-native environment.

Each selected tool plays a distinct role in the system's architecture.

1. For OCR, it's the Google Vision API.
 - ***Its job is to:*** Converting scanned documents and images into machine-readable text with high accuracy.
 - ***Why this tool?*** It was chosen because of its enterprise-grade accuracy, multilingual support, and native integration.
 - ***Why not others?*** Open-source tools like Tesseract OCR require significant maintenance and tuning, and commercial alternatives like ABBYY FineReader come with high licensing costs and integration challenges.
2. For document classification: Vertex AI.
 - ***Its job is to:*** Train and deploy a custom machine learning model that automatically classifies documents and extracts metadata according to the ISO 23081 schema.

- **Why this?** It enables the creation of classification rules tailored to SGU's specific needs within a secure, integrated environment.
 - **Why not others?** Although competing cloud platforms like AWS Comprehend and Azure Form Recognizer are technically capable, they would introduce significant security and integration challenges into SGU's Google-centric ecosystem.
3. For semantic search and Q&A: Gemini AI.
- **Its job is to:** To provide a conversational interface that allows users to ask questions of complex documents, such as contracts and policies. This enables deep understanding and fast, accurate information retrieval.
 - **Why this?** Gemini AI offers advanced semantic capabilities and native Google Workspace integration, ensuring data privacy and compliance.
 - **Why not others?** Alternatives like OpenAI's GPT-4 or Microsoft Copilot are not native to the SGU environment, raising critical concerns about data privacy, compliance, and interoperability.

This integrated stack of Google-native AI tools provides the optimal balance of advanced functionality, security, cost-effectiveness, and practical deploy ability for this proof of concept (PoC). The following table provides a condensed summary of this comparative evaluation.

Table 2.4 Comparative Evaluation of AI Tools for the Proposed System

Function	Tool	Key Strengths	Limitations	Inclusion / Exclusion Rationale
OCR (Optical Character Recognition)	Google Vision API	High OCR accuracy, layout-aware, supports handwriting, strong multilingual support, native Google Workspace integration (<i>Cloud Vision API documentation</i> , 2024).	Limited semantic structuring in output	Included: Aligns with SGU's GWS-E ecosystem, reduces integration effort, scalable for enterprise needs
	Tesseract OCR (Open Source)	Free, customizable, wide language support (Reul <i>et al.</i> , 2019).	Requires local deployment, complex tuning for	Excluded: Not cloud-native, high maintenance overhead

Function	Tool	Key Strengths	Limitations	Inclusion / Exclusion Rationale
			layouts, lacks enterprise security	
	ABBYY FineReader	High accuracy for complex documents, form/table recognition (Reul <i>et al.</i> , 2019).	High licensing cost, lacks native GWS integration	Excluded: Adds cost and complexity without native interoperability
Document Classification & Metadata Extraction	Vertex AI (Custom Model)	Custom ML model training/deployment, AutoML support, secure GCP hosting (Choi, Choi and Heo, 2023).	Requires initial training data and ML expertise	Included: Enables tailored classification aligned with ISO 23081 metadata governance; minimal integration friction
	AWS Comprehend	Entity recognition, text analytics (Choi, Choi and Heo, 2023).	Complex IAM setup, external to GWS	Excluded: Security and integration overheads
	Azure Form Recognizer	Strong form/table data extraction (Choi, Choi and Heo, 2023).	Best suited for structured docs; MS-centric	Excluded: Not optimal for GWS-based workflow
Semantic Search & Conversational Q&A	Gemini AI	Context-aware Q&A, semantic search, native GWS integration, private data support (Qi <i>et al.</i> , 2023).	Pretrained, limited fine-tuning, explainability constraints	Included: Meets SGU's deep document understanding needs, maintains compliance with COBIT/ISO standards
	NotebookLM	Personalized Q&A with citations (Tufino, 2025).	Manual doc upload, lacks real-time scalability	Excluded: Not suited for dynamic document flows
	OpenAI GPT-4	Advanced reasoning and generation (Qi <i>et al.</i> , 2023).	Privacy risks, external hosting, not GWS-native	Excluded: Fails SGU's compliance and integration requirements
	Microsoft Copilot	Deep MS Office integration (Microsoft, 2025).	Requires Microsoft 365 environment	Excluded: Incompatible with GWS-based infrastructure

2.7 Cloud Computing and Google Workspace for Education Plus

The widespread adoption of cloud computing has fundamentally reshaped IT infrastructure and service delivery in all sectors, including higher education. This technology has transformed the operational models of higher education institutions (HEIs), enabling greater scalability, collaboration, and cost efficiency. This section

critically examines the foundational concepts of cloud computing, its advantages and challenges, and the rationale for selecting **Google Workspace for Education Plus (GWS-E+)** as the cloud platform for the proposed intelligent document governance system at SGU. The Plus tier was chosen because of its advanced security features, expanded compliance requirement, and native integration with AI tools, all of which are necessary to solve the problems mentioned in Chapter 1.

2.7.1 Understanding Cloud Computing

Cloud computing represents a paradigm shift in how computing resources are accessed and utilized. Rather than using on-premises infrastructure, it provides on-demand services via the internet (*"the cloud"*) under flexible, pay-as-you-go pricing models (Mell and Grance, 2011). According to the National Institute of Standards and Technology (NIST), there are five key characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Cloud services are delivered through three main models:

- **Software as a Service (SaaS):** In this model, entire applications are hosted and managed by providers and accessed via a web browser (e.g., Google Workspace or Salesforce).
- **Platform as a Service (PaaS):** This model provides a development and deployment environment without the complexity of managing the underlying infrastructure (e.g., Google App Engine).
- **Infrastructure as a Service (IaaS):** The provision of fundamental computing resources, such as virtual machines and storage, which gives users a high level of control (e.g., Google Compute Engine).

Deployment models include public cloud (shared services over the internet), private cloud (exclusive to one organization), and hybrid cloud (a combination of both) (Mell and Grance, 2011). Higher education institutions often choose cloud platforms for their flexibility, scalability, and cost-effectiveness (Almajalid, 2017).

2.7.2 Benefits and Challenges of Cloud Computing Adoption

Higher education institutions that adopt cloud computing enjoy a range of transformative benefits that extend beyond technical efficiency and influence how teaching, research, and administration are conducted. One of its most notable advantages is **scalability and elasticity**, which enable institutions to adjust their computing resources dynamically to meet fluctuating demands, such as during peak loads for admissions or examinations (Mell and Grance, 2011). This flexibility is complemented by **cost efficiency** as the cloud transforms capital expenditures into operational expenditures through pay-as-you-go models, thereby reducing initial investments and ongoing maintenance costs (Almajalid, 2017).

The anywhere **accessibility and enhanced collaboration** that cloud platforms provide are equally important. Faculty, students, and administrative staff can access systems and resources from any internet-connected device, enabling seamless learning, distributed research activities, and greater operational flexibility (H. *et al.*, 2017). Furthermore, cloud infrastructures offer **high reliability and disaster recovery requirement**. They leverage providers' robust global infrastructures to deliver superior uptime and data protection compared to typical on-premises solutions (Al-Malah *et al.*, 2021). By managing infrastructure maintenance, security updates, and patches, providers help institutions **reduce IT management overhead**, allowing internal teams to focus on more strategic initiatives that add value (Al-Malah *et al.*, 2021).

Despite the benefits of cloud adoption, it introduces a set of challenges, particularly concerning **security and risk management**. According to the shared responsibility model, providers secure the underlying cloud infrastructure, but the institution is responsible for safeguarding data, managing access controls, and ensuring compliance (Anak Bangkong, Ehsan Rana and Hameed, 2023). These responsibilities are closely tied to **data sovereignty and compliance requirements**, necessitating adherence to Indonesia's Personal Data Protection Law and applicable international regulations, such as the GDPR.

Another concern is **vendor lock-in**, since migrating large datasets and integrated systems between providers can be technically complex and financially burdensome (Almajalid, 2017). Institutions must also contend with **internet dependence** since service availability depends on stable connectivity. Any outage can disrupt operations and hinder access to critical systems (Al-Malah *et al.*, 2021). Finally, **cost management** is an ongoing challenge because the flexible nature of cloud billing can lead to escalating expenses without proper governance and optimization practices (Mell and Grance, 2011).

In short, cloud computing empowers higher education institutions (HEIs) with unprecedented scalability, cost efficiency, and collaborative requirement. However, the successful adoption of cloud computing depends on robust governance, risk mitigation, and compliance strategies. These themes are directly relevant to the design and implementation of SGU's intelligent document governance system.

2.7.3 Google Workspace for Education Plus (GWS-E+) as the Chosen Platform and its Security Posture

Google Workspace for Education Plus (GWS-E+) is the most advanced tier of Google's cloud suite focused on education. It serves as the foundation for the proposed intelligent document governance system at SGU. Based on the core Google Workspace applications, including Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, and Classroom, the Plus edition provides enhanced security, advanced analytics, and premium administrative controls (details comparison of Google Workspace presented in Appendix A). These requirement are delivered through Google's globally distributed and resilient cloud infrastructure, which powers mission-critical services like Google Search and YouTube (Workspace, 2021).

The decision to select GWS-E+ was strategic and pragmatic, emerging from a critical evaluation of SGU's operational requirements, security concerns, and existing infrastructure. **SGU has already adopted Google Workspace for its daily operations**, so the platform is a natural choice that minimizes the learning curve and reduces resistance to change. Faculty, staff, and students are already familiar with the

interface and workflows, so the new system will be adopted more smoothly without the cultural or training overhead often associated with platform transitions.

As a cloud-native solution, GWS-E+ is inherently **scalable**, accommodating the university's growing data volume and user base. It provides high service availability and fault tolerance to ensure that mission-critical academic and administrative processes remain uninterrupted. GWS-E+ natively integrates with Google Cloud's artificial intelligence and machine learning services, including Google Document AI, Vertex AI, and advanced semantic search requirement. This deep integration reduces development complexity and enables the creation of AI-powered features within a secure, familiar environment, which is a central requirement of this research.

From a collaboration standpoint, GWS-E+ directly addresses SGU's knowledge fragmentation issues by fostering unified document creation and real-time co-authoring. Tools such as Google Docs, Sheets, and Drive streamline workflows by eliminating siloed document storage and reducing operational inefficiencies. These requirements closely align with the governance and productivity improvements sought in the proposed system.

Security and compliance are both critical factors in this decision. Under the shared responsibility model, Google secures its cloud infrastructure, including data centre networking, and core services, while institutions manage data classification, access control, and internal policies. GWS-E+ helps SGU meet its compliance obligations with a robust security architecture incorporating multi-layered defences and AI-powered threat detection that blocks over 99.9% of spam, phishing, and malware. It also has context-aware access controls (Workspace, 2021). Furthermore, **GWS-E+ grants institutions full data ownership and intellectual property rights**, explicitly stating that Google does not use data from core education services for advertising purposes.

GWS-E+ meets a wide range of **international and sector-specific certifications and compliance standards**, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, FERPA, and GDPR. These certifications are maintained through regular independent

audits. This external validation provides assurance to SGU stakeholders and mitigates the heightened compliance risks identified in Chapter 1. Additional built-in features, such as data loss prevention (DLP), advanced identity and access management (IAM) with multi-factor authentication, Google Vault for eDiscovery and legal holds, and an advanced security centre dashboard, enable SGU to maintain control over its "*security in the cloud*" responsibilities.

Finally, the GWS-E+ offers an **extensive API ecosystem** that supports custom development and interoperability with other systems. This flexibility allows the intelligent document governance system to seamlessly integrate additional modules, automate workflows, and interface with SGU's broader IT ecosystem.

SGU's selection of Google Workspace for Education Plus (GWS-E+) as the foundation for its intelligent document governance system is based on GWS-E+'s proven reliability, advanced collaboration requirement, robust security, and integration with Google Cloud's AI ecosystem. This alignment ensures that the proposed system addresses the operational and compliance challenges identified in Chapter 1 and leverages existing institutional familiarity to maximize adoption success. Table 2.6 aligns each core institutional need with the GWS-E+ requirement that enable the functional, governance, and AI-driven objectives of this research.

Table 2.5 Strategic Fit of GWS-E+ with SGU's Intelligent Document Governance System

SGU Problem / Need (from Chapter 1)	Relevant GWS-E+ Requirement	Strategic Benefit to the Proposed System
Operational inefficiencies and fragmented knowledge management	Integrated suite of collaborative tools (Docs, Drive, Sheets, Apps Script)	Enables real-time collaboration and unified document creation, reducing workflow fragmentation and fostering a cohesive information environment.
Heightened compliance risks and data security concerns	Robust security architecture and compliance certifications (ISO 27001, ISO 27017, ISO 27018, FERPA, GDPR)	Provides industry-validated security measures, ensures SGU retains full data ownership, and mitigates compliance risks through external certification.
Heightened compliance risks and data security concerns	Built-in security controls (DLP, IAM with MFA, context-aware access, Vault, Security Center)	Empowers SGU to manage " <i>security in the cloud</i> " with granular access controls, prevention of data loss, and support for eDiscovery and legal holds.

SGU Problem / Need (from Chapter 1)	Relevant GWS-E+ Requirement	Strategic Benefit to the Proposed System
Requirement for AI-enhanced document and contract governance	Native integration with Google Cloud AI (Document AI, Vertex AI, semantic search)	Simplifies development of intelligent features such as automated classification and metadata extraction, reducing integration complexity and technical risk.
Existing infrastructure and adoption barriers	Widespread institutional adoption of GWS-E+	Minimizes user learning curve, reduces change resistance, and leverages an established operational ecosystem for faster, smoother implementation.
Need for scalability and cost-effectiveness	Cloud-native architecture with on-demand scalability and OpEx pricing model	Accommodates growing data volumes and user demand without significant capital investment, supporting sustainable long-term operations.
Requirement for well-integrated institutional IT ecosystem	Extensive API ecosystem for system interoperability	Supports seamless integration with other SGU systems, enabling automation and ensuring the governance system operates within the broader IT architecture.

As shown in Table 2.5, GWS-E+ uniquely combines collaborative efficiency, governance control, and AI readiness within a single, cloud-native environment. By aligning SGU's operational priorities with the platform's embedded requirement, the proposed system minimizes technical integration risks and accelerates implementation. The platform's compliance certifications (e.g., ISO 27001, ISO 27017, ISO 27018, FERPA, and GDPR) and built-in security controls ensure that governance, risk management, and compliance (GRC) requirements derived from COBIT 2019, ISO 15489, and ISO 23081 are embedded in the system's architecture from the beginning. This strategic fit reinforces the feasibility of developing an AI-enhanced governance system that is both technically robust and institutionally sustainable.

2.8 Research Methodologies and Development Approaches in Information Systems Literature

This research is based on four complementary components: 1) Design Science Research (DSR) as the overarching research paradigm; 2) an iterative/Agile System Development Life Cycle (SDLC) as the development framework; 3) prototyping as the operational mechanism for iterative delivery; and 4) the Architecture Development Method (ADM) of The Open Group Architecture Framework (TOGAF) Phases B–D as the architectural guideline. These approaches ensure the system is designed, developed, and refined in a

structured yet adaptive manner. This enables early validation and stakeholder feedback while preserving architectural coherence.

2.8.1 Design Science Research (DSR) Paradigm

Design science research (DSR) is a problem-solving paradigm in information systems research. It focuses on designing, building, and evaluating artifacts, such as systems, models, or processes, to address real-world challenges while contributing to theoretical knowledge (Hevner *et al.*, 2004; Peffers, Tuunanen and Niehaves, 2018). DSR emphasizes two simultaneous outcomes: a practical artifact that solves an identified problem and a scholarly contribution to the knowledge base.

The DSR process comprises six iterative stages, as outlined by Peffers et al. (2018): problem identification, objective definition, artifact design and development, demonstration, evaluation, and communication. Hevner's three-cycle model reinforces this by linking the relevance cycle (connection to the problem environment), the rigor cycle (link to existing knowledge), and the design cycle (iterative artifact creation and evaluation) (Hevner, 2007), as shown in figure 2.5 below. In the context of this study, these cycles ensure that the AI-enhanced document governance system for SGU is problem-driven, informed by existing standards (ISO 15489, ISO 23081, COBIT), and refined through real-world testing.

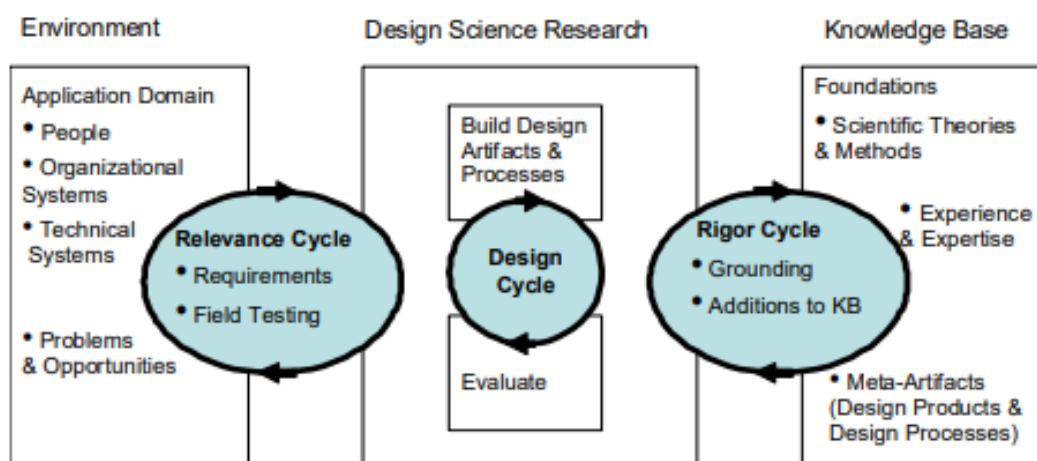


Figure 2.5 Design Science Research Three-Cycle Framework
Source: (Hevner, 2007)

2.8.1.1 Justification for Selecting DSR

This research adopts the **Design Science Research (DSR)** paradigm, specifically, the research process is structured and guided by **Hevner's three-cycle model**, which links the relevance of the problem, the rigor of the knowledge base, and the iterative design of the artifact.

Alternative Methodologies Considered:

- **Action Research (AR):** Action research emphasizes collaborative problem-solving within a specific organizational context. Researchers and practitioners collaborate to diagnose a problem, plan an intervention, implement it, and reflect on its outcomes (Avison *et al.*, 1999). Although action research is cyclical and participatory and aims to have a practical impact, its primary focus is localized organizational change and learning within a specific context, rather than creating generalizable artifacts. In this study, SGU is a specific case; however, the ultimate goal is to produce a transferable system and derive recommendations applicable to other higher education institutions. This goal is less central to the core contribution of AR.
- **Case Study Research:** According to Coombs (2022), case study research involves an in-depth, empirical investigation of a contemporary phenomenon within its real-world context, especially when the boundaries between the phenomenon and its context are unclear (Coombs, 2022). This methodology is highly effective for exploratory or descriptive purposes, providing a rich contextual understanding of complex situations. However, case study research is fundamentally limited because it is primarily an observational and analytical methodology. It lacks the artifact creation and prescriptive focus that are central to DSR. While this study uses SGU as a demonstration and evaluation case, its core activity is developing a solution rather than observing an existing one.
- **Empirical/Behavioural Research:** This category includes experimental, survey, and quasi-experimental methodologies. These methodologies focus on testing theories by collecting and analyzing quantitative or qualitative data. They often aim to confirm or refute hypotheses about behavior, system use, or

relationships between variables (Weathington, Cunningham and Pittenger, 2017). These methods provide valuable insights into user perceptions, system impacts, and specific phenomena. However, they are insufficient for projects primarily focused on creating a new system or artifact because they do not involve the systematic design and development processes inherent in this type of research.

DSR was chosen because it is the only methodology that provides a systematic and rigorous process for solving practical problems through artifact design and generating generalizable knowledge from that process.

The following table summarizes the comparative analysis of these methodologies.

Table 2.6 Comparison of Research Methodologies

Methodology	Focus Area	Strengths	Limitation vs. DSR
Design Science Research	Artifact creation & evaluation to solve real-world problems	Produces generalizable artifacts; bridges theory and practice; iterative and problem-driven	Requires balancing theoretical rigor with practical relevance; resource-intensive
Action Research	Collaborative problem-solving & organizational change	Context-specific solutions; fosters direct organizational learning	Localized outcomes; weaker theoretical generalizability
Case Study Research	In-depth investigation in context	Rich contextual insights; suitable for exploratory work	Primarily observational; no systematic artifact creation
Empirical Research	Theory testing via data collection	Strong predictive and statistical validation; useful for evaluation	Does not produce artifacts; not suited for design-focused research

2.8.1.2 Application of DSR in This Research

The DSR paradigm provides the overarching structure for this thesis. In this project, the specific "job" of DSR is to:

- **Guide the Research Process:** Research activities are structured around Hevner's three-cycle framework. The Relevance Cycle connects research to real-world problems at SGU (as defined in Chapter 1). The Rigor Cycle grounds the design of artifacts in existing knowledge (Chapter 2). The central Design Cycle guides the iterative creation and evaluation of artifacts (Chapters 3 and 4).

- **Ensure Rigor and Relevance:** The methodology grounds the research in a real-world problem at SGU (the relevance cycle) and informs it with existing theories and frameworks from the literature (the rigor cycle).
- **Structure the Core Contribution:** The DSR framework positions the final artifact, the proof of concept (PoC) system, and the resulting design principles as tangible contributions to practice and academic knowledge.

2.8.2 System Development Life Cycle (SDLC) Approaches

While the Design Science Research (DSR) paradigm guides the overall research process, a specific **System Development Life Cycle (SDLC)** model is needed to manage the technical design and implementation of the artifact. This research adopts an **Iterative/Agile SDLC model** to structure the development of the Proof-of-Concept.

The SDLC provides a structured pathway for translating requirements into a functional system. This process typically involves planning, analysis, design, implementation, testing, and maintenance stages (Radack, 2009). Agile/iterative models adapt these stages into shorter cycles that emphasize flexibility, rapid feedback, and continuous improvement. This phase illustrated in figure 2.6.

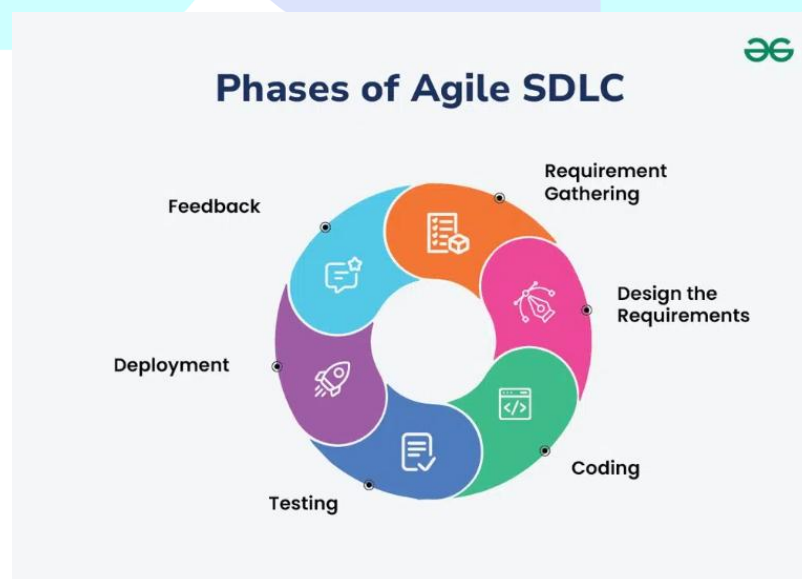


Figure 2.6 Agile SDLC Phases
Source: (GeeksforGeeks, 2025)

2.8.2.1 Justification for Selecting an Iterative/Agile SDLC

The choice of an iterative/agile approach is based on the specific needs of a DSR project involving prototyping and experimentation with AI components. A comparative analysis of traditional models confirms this choice.

Alternative models considered:

- The Waterfall model is too rigid due to its linear and sequential structure. It does not allow for the flexibility needed to refine requirements or adapt the design based on early feedback, which is crucial for this proof of concept (PoC).
- The spiral and V models, while offering more structure around risk and testing, are too complex for a time-bound academic prototype and less suited to managing the evolving nature of AI tool integration.

Therefore, the iterative/agile model was selected because it best supports the core activities of this research: rapid prototyping, incorporating user feedback from SGU stakeholders, and experimentation with AI components. The following table summarizes this comparative analysis.

Table 2.7 Comparison of SDLC Model

SDLC Model	Characteristics	Strengths	Limitation for This Study
Iterative/Agile	Flexible, user-centric, rapid cycles	Supports prototyping, fast feedback	Requires active stakeholder participation
Waterfall	Linear, sequential	Simple, predictable	Inflexible, late feedback
Spiral	Iterative with risk focus	Strong risk management	High complexity, not ideal for a prototype
V-Model	Paired development and testing	Quality-focused, structured	Less adaptive, not ideal for evolving AI

2.8.2.2 Application of the Iterative/Agile SDLC in This Research

The Iterative/Agile model provides a framework for executing the technical aspects of the project. This SDLC model's specific "job" is to:

- **Structure the development sprints:** The development process is broken down into short, iterative cycles, each of which focuses on building and testing a specific feature (e.g., OCR, automated classification, or contract alerts).

- ***Facilitate early feedback:*** This approach allowed the research team to present functional parts of the prototype to SGU's HR and finance departments early in the process. Their feedback guided subsequent development cycles.
- ***Manage AI experimentation:*** The model provided the flexibility to test and refine the integration of different Google AI tools, adapting the approach as their capabilities and limitations became clearer.

Embedding these Agile principles within the DSR framework ensures that the final artifact is technically functional and closely aligned with the real-world needs of its end users.

2.8.3 Prototyping in Applied Information Systems Research

Prototyping is a fundamental method in design science research (DSR) and applied information systems development. It bridges the gap between theoretical constructs and practical implementations. Prototyping plays a critical role in validating technical feasibility, clarifying and refining requirements, and mitigating design risks early in the development process (Hevner *et al.*, 2004; Venable, Pries-Heje and Baskerville, 2016). Iterative prototyping facilitates a dynamic learning cycle, enabling successive enhancements to the artifact and fostering alignment with stakeholder needs and governance frameworks.

Within the DSR paradigm, prototyping is a central mechanism in the artifact evolution process, stimulating design reflection, enhancing artifact quality, and reinforcing the relevance of research outcomes (Peffers *et al.*, 2007). Integrating prototyping into an iterative or Agile software development life cycle (SDLC) framework enables researchers to maintain architectural discipline (e.g., adherence to the Open Group Architecture Framework (TOGAF) Architecture Development Method (ADM)) while embracing the flexibility necessary to adapt to emergent requirements in practice settings, especially those involving AI-driven tools.

2.8.3.1 Justification for a PoC Prototyping Approach

Developing a proof of concept (PoC) rather than a full-scale, production-ready system is a strategic choice that aligns with the objectives of a Master's thesis and the principles of distributed systems (DSR).

- **Why a prototype?** Prototyping is essential in DSR because it bridges the gap between theoretical design and practical application. It enables the validation of technical feasibility, clarification of user requirements, and mitigation of design risks early in the process (Hevner *et al.*, 2004).
- **Why a PoC?** A proof of concept is the most appropriate form of prototype for this research. Its primary goal is not to deliver a complete enterprise system but rather to demonstrate the viability and potential value of the proposed integrated framework. This approach manages the project's scope, contains costs, and provides a validated model that could justify a larger-scale implementation at SGU in the future.

2.8.3.2 Application of Prototype in This Research

The PoC developed in this research has a clearly defined, limited scope. Its specific purpose is to validate the core functionalities derived from the research objectives; it is not intended to be a comprehensive enterprise solution. The prototype is intentionally focused on demonstrating:

- **Governance of Finalized Documents:** The system will demonstrate how finalized administrative documents can be securely stored with consistent, AI-generated metadata in a centralized repository, thereby illustrating the core principles of ISO 15489 and 23081.
- **Automated Contract Renewal Alerts:** The prototype will show how to track contract expiration dates using metadata and trigger automated notifications. This validates a key business requirement without the need to develop a comprehensive contract lifecycle management system.

Situating this focused proof of concept (PoC) within the DSR and Agile frameworks effectively balances methodological rigor with practical innovation, setting the stage for the detailed methodology presented in Chapter 3.

2.9 Approaches to System Evaluation and Validation in Information Systems Literature

In information systems research, effectiveness encompasses technical performance, user experience, likelihood of adoption, and alignment with organizational objectives. The literature on human-computer interaction (HCI), information systems (IS), and IT governance consistently emphasizes the importance of combining usability evaluation and system requirement validation to ensure user satisfaction and institutional value (Davis, 1989; Nielsen, 1994; *COBIT | Control Objectives for Information Technologies*, 2019).

Building on these principles, this study's evaluation and validation strategy is designed to ensure that the developed proof-of-concept (PoC) system for AI-enhanced document and contract governance at SGU meets practical effectiveness and theoretical rigor standards. This approach integrates usability evaluation, system validation, and AI-specific performance assessment. It is framed by the following governance and development standards: TOGAF ADM Phases B–D, COBIT 2019, ISO 15489, ISO 23081, Design Science Research (DSR), and an Iterative/Agile System Development Life Cycle (SDLC).

This dual-lens approach distinguishes **usability evaluation**, which examines the system from the user's perspective focusing on ease of use, efficiency, and satisfaction, from **system validation**, which assesses conformance to functional, technical, and governance requirements. Using both methods ensures alignment with the Design Science Research (DSR) relevance cycle (which addresses real-world institutional problems), the DSR rigor cycle (which links development to established theory and standards), and the DSR design cycle (which enables iterative refinement through user and expert feedback). This alignment guarantees that the evaluation outcomes measure technical success and demonstrate the system's ability to support governance, compliance, and operational objectives in the management of higher education documents.

2.9.1 Usability Evaluation in Informatic Systems

Both academic theory and practical implementation acknowledge that usability is a critical factor in the success of a system. In organizational and educational contexts, high usability is linked to user acceptance, task efficiency, and long-term sustainability (Davis, 1989; Nielsen, 1994). In information systems research, especially in document governance in higher education, usability evaluations ensure that newly introduced systems are functional, intuitive, efficient, and valuable to end users.

This research focuses on the potential adoption of the PoC system within SGU's HR and Finance departments, where the primary users are administrative staff. Consistent with human-computer interaction (HCI) and IT governance literature, this study adopts a triangulated approach combining standardized quantitative measures, performance-based testing, and qualitative user feedback (Brooke, 1996; Hollender *et al.*, 2010; Strijker, Bosworth and Bouter, 2020)). This approach enables the measurement of both perceived and actual usability and supports iterative refinement in line with DSR's design cycle.

2.9.1.1 System Usability Scale (SUS)

The System Usability Scale (SUS), developed by Brooke (1996), is one of the most widely used instruments for measuring perceived usability. Consisting of a 10-item Likert scale, it is designed to capture users' subjective evaluation of a system's ease of use, consistency, and learnability (Brooke, 1996). Theoretically, the SUS is based on the Technology Acceptance Model (TAM), which states that perceived ease of use and perceived usefulness are the two main predictors of a user's intention to use a system (Davis, 1989). The SUS directly measures these constructs by asking users to rate their interaction experience, thereby providing a quantifiable proxy for user acceptance. A SUS score of 70 or above is generally considered to indicate acceptable usability and is often used as a benchmark in system evaluation studies.

Justification for Selecting SUS: SUS was selected because it is a robust, reliable, and industry-standard tool for measuring perceived usability. Although other usability metrics exist, the SUS was chosen for three key reasons:

- *Reliability and validity:* SUS is a well-established and extensively validated "quick and dirty" usability scale. Its 10-item questionnaire has been proven to produce reliable results across a wide range of systems and contexts.
- *Industry Benchmark:* SUS provides a single, easily understood score from 0 to 100. This score can be compared to a widely accepted industry benchmark where a score above 68 is considered above average. This provides a clear, objective measure of success.
- *Focus on Perceived Usability:* The scale directly measures users' subjective perception of ease of use. This aligns perfectly with the need for research to gauge user acceptance and address potential resistance to new tools at SGU, as highlighted in the Technology Acceptance Model (TAM).

Application of SUS in This Research: During the evaluation phase of this DSR project, the SUS plays a very specific and critical role. It is not just a general feedback tool, but rather the primary instrument for:

- *Quantitative Usability Measurement:* The SUS will be administered to the user testing group at SGU to generate a quantifiable score representing the PoC's overall usability.
- *Empirical Hypothesis Testing:* The resulting SUS score will serve as the core empirical data used to evaluate and validate hypothesis 4 (H4), which posits that the prototype will achieve high usability scores.

Using a standardized, widely respected instrument like the SUS ensures that the evaluation of the artifact is rigorous and directly comparable to established usability benchmarks.

2.9.1.2 Task-Based Testing

While the System Usability Scale (SUS) measures perceived usability, task-based testing evaluates actual usability through observable performance. This method objectively assesses how efficiently and effectively users can complete specific tasks within the system, moving beyond subjective opinions. Users are asked to complete

predefined tasks, such as uploading a document, retrieving a contract, or triggering a deadline reminder, while metrics such as task success rate, completion time, and error frequency are recorded. This method is widely supported in **HCI research** for assessing system efficiency, error tolerance, and learnability in real-world contexts (Hollender *et al.*, 2010). Metrics include:

- $\geq 80\%$ task completion rate for critical functions
- ≤ 2 errors per critical task
- Completion time within predefined benchmarks

Justification for Using Task-Based Testing: Including task-based testing is critical for a complete evaluation of the artifact. While the System Usability Scale (SUS) asks, "Do users feel the system is easy to use?" task-based testing asks, "Can users actually complete their work efficiently and effectively with the system?".

- *Complement to SUS:* This method provides objective performance data to validate subjective SUS feedback. A high SUS score combined with high task success rates is powerful evidence of a successful design.
- *Focus on Efficiency and Effectiveness:* In SGU's administrative context, efficiency is a key requirement. Task-based testing directly measures performance metrics such as task success rate, error frequency, and completion time. These metrics are crucial for determining whether the system improves operational workflows.
- *Direct Link to Functional Requirements:* This method enables direct testing of the system's core functionalities against specific identified problems (e.g., can a user find a specific contract within a target time?).

Application of Task-Based Testing in This Research: During the evaluation phase, task-based testing plays a precise and practical role. It is the primary instrument for objective performance measurement:

- *Objective Performance Measurement:* User from SGU's HR and Finance departments will be asked to complete a set of predefined, realistic tasks (e.g.,

upload a contract, find a policy, or check a renewal date). Their performance will be observed and measured.

- *Validating Operational Improvement:* The gathered data (e.g., achieving an 80% or higher task completion rate) will be used to empirically assess whether the prototype effectively addresses the operational inefficiencies identified in Research Question 1 (RQ1).
- *Providing Diagnostic Feedback:* Unlike a single SUS score, observing where users fail or struggle during tasks provides specific, actionable feedback that can inform recommendations for future development and full-scale implementation.

2.9.1.3 Qualitative Feedback

Although quantitative metrics (e.g., SUS scores or task completion times) are essential, they may not fully capture nuanced user perceptions or emotional responses. These metrics also fail to reveal less visible interface problems and unmet needs. Therefore, qualitative feedback gathered through methods such as structured interviews, open-ended survey responses, and guided discussions (e.g., focus group discussions) is essential for gaining a deeper understanding of user attitudes, frustrations, suggestions for improvement, and the overall context of their interaction with the system (Strijker, Bosworth and Bouter, 2020). This approach is based on the idea that the user experience is multifaceted and goes beyond measurable performance to include subjective feelings and cognitive processes (Strijker, Bosworth and Bouter, 2020). These techniques offer valuable diagnostic insight into how the system can be improved to better support real-world use and user satisfaction.

Justification for Using Qualitative Methods: Including qualitative methods is crucial for a holistic evaluation. Quantitative data alone is insufficient because it may overlook nuanced user perceptions, frustrations, and valuable suggestions for improvement.

- *Qualitative feedback complements quantitative data:* Qualitative feedback gathered through structured interviews and open-ended questions provides the contextual narrative needed to interpret quantitative scores. It helps explain a

low task-success rate or a mediocre SUS score, turning numbers into actionable insights.

- *Diagnostic Power:* This approach has unparalleled diagnostic power for uncovering specific usability problems, understanding user mental models, and identifying unmet needs that would not be visible in performance data alone.
- *Focus on User Acceptance:* For a system intended for non-technical users at SGU, it is vital to understand their subjective feelings and cognitive processes to ensure user acceptance and minimize resistance during a potential future rollout.

Application of Qualitative Feedback in This Research: During the evaluation phase, qualitative feedback plays a specific diagnostic role. It is the primary instrument for:

- *Explaining the "why":* Qualitative data will be collected through post-testing interviews and open-ended survey questions to understand the reasons behind the observed quantitative results.
- *Identifying specific usability issues:* User comments will be analysed to pinpoint pain points in the user interface or workflow that need improvement.
- *Gathering recommendations for future work:* This method is the primary source for gathering user-generated ideas and suggestions that will directly inform the recommendations for the full-scale system in Chapter 5.

Combining these three evaluation methods—SUS (perception), task-based testing (performance), and qualitative feedback (context)—ensures a robust, mixed-methods approach and a comprehensive, insightful assessment of the artifact.

2.9.1.4 Usability as a Governance Requirement

Finally, it is important to note that, in this research, usability is not considered an isolated user experience (UX) metric, but rather a core, governance-aligned requirement. The selected IT governance and records management frameworks implicitly or explicitly require usability for compliance and effectiveness. If a system is difficult to use, users will circumvent it, which can lead to governance failures, such as information silos and noncompliance.

The connection is clear across the selected frameworks:

- **COBIT 2019:** COBIT 2019 links system adoption to value delivery and risk management. A system with poor usability risks low adoption, failing to deliver its intended value and return on investment.
- **ISO 15489:** ISO 15489 requires that records be accessible and usable. A system with a confusing interface or inefficient workflow violates this principle because it hinders authorized users from efficiently locating and using the records they need.
- **ISO 23081:** ISO 23081 emphasizes that the primary purpose of metadata is to make records findable and understandable. Therefore, a system that does not present this metadata clearly and intuitively fails to meet the standard's objective.

Application in This Research: This study elevates the role of the evaluation by integrating these perspectives. The results of the usability tests (SUS, task-based testing, and qualitative feedback) will be more than just UX feedback. Rather, they will be interpreted as direct evidence of the system's ability to meet the governance objectives established by COBIT and ISO standards. This approach ensures the artifact's design is assessed holistically, balancing technical functionality with human-centric factors essential for sustainable adoption and long-term institutional compliance.

2.9.2 System Validation in Design Science and Applied Research

In information systems research, system validation focuses on determining whether a developed artifact meets the functional, technical, and governance requirements established during the design phase. It also demonstrates the artifact's institutional relevance and strategic fit. Unlike usability evaluations, which assess systems from an end-user perspective, validations examine whether implemented features, workflows, and controls fulfil their intended purposes in alignment with organizational goals and compliance standards (Hevner *et al.*, 2004; Gregor and Hevner, 2013).

In this study, validating the AI-enhanced document and contract governance proof of concept (PoC) system for Swiss German University (SGU) is essential to ensure it operates as intended and adheres to recognized governance and records management standards. These standards include The Open Group Architecture Framework (TOGAF) ADM Phases B–D, Control Objectives for Information and Related Technology (COBIT) 2019, ISO 15489 and ISO 23081. This multi-layered approach enables evaluation of the system's technical performance, compliance, and contextual fit within SGU's institutional environment.

2.9.2.1 Functional Requirements Validation

Functional requirements validation is a critical step in information systems development, ensuring that the implemented features operate in accordance with the specifications defined during the design phase and meet the intended organizational objectives (*Understanding Requirements Validation in Business Analysis*, 2025). It answers the fundamental question: "*Does the system do what it was designed to do?*".

This process explicitly links the technical implementation to the guiding frameworks by verifying that the application components (TOGAF Phase D) correctly implement the ISO and COBIT standards and successfully deliver the business and data requirements (Phases B and C).

Application of Functional Validation in This Research: The validation process involves executing a series of predefined test scenarios that reflect SGU's real-world use cases. This validation confirms the error-free execution of the four core functionalities:

- ***Document Upload:*** The ability to receive and store final, authorized documents in a secure and structured repository.
- ***Automated OCR Processing via Google Vision API:*** Accurate conversion of scanned or image-based documents into machine-readable text for indexing and search (Workspace, 2021).
- ***AI-Based Metadata Classification using Vertex AI:*** Automatic tagging of documents with standardized metadata attributes (e.g., document type,

department, effective dates) to support retrieval and governance (*ISO 23081-1:2017*, 2023).

- ***Contract Renewal Notifications via Google Calendar Integration:*** Automated reminders for contract expiration dates, ensuring proactive compliance with institutional timelines.

This validation process confirms that each of these core functions meets its architectural specification. This ensures that the proof of concept (PoC) is technically sound and provides the necessary foundation for subsequent usability evaluations. Chapter 3 will detail the specific success criteria and test scenarios for each function.

2.9.2.2 Scenario-Based Simulation

Scenario-based simulation, also known as use-case simulation, is a practical evaluation method commonly employed in applied information systems (IS) research. It assesses how a system performs under realistic operational conditions (Hevner *et al.*, 2004; Yin and McKay, 2018). It involves designing and executing test scenarios that replicate specific institutional workflows. This enables researchers to observe system behaviour, verify feature integration, and assess problem-solving capacity in situations that closely reflect real-world use.

Justification for Using Scenario-Based Simulation: This evaluation method is essential for demonstrating the practical value of the system and its ability to solve complex, multi-step problems identified at SGU.

- ***Holistic Workflow Validation:*** Unlike testing isolated functions, scenario-based simulations assess the entire process chain, including document upload, AI processing, and final retrieval and notification. This is critical for verifying the successful integration of all system components, such as Google AppSheet, Vision AI, and Vertex AI.
- ***Contextual Realism:*** Designing test scenarios that replicate specific SGU workflows (e.g., *"An HR staff member needs to find an expiring contract for a*

lecturer") provides strong evidence that the system can perform effectively in its intended real-world environment.

- *Direct Link to Problem-Solving*: This approach directly tests the system's capacity to solve the specific, fragmented process challenges identified in Research Question 1 (RQ1), moving beyond feature testing to problem validation.

Application of Scenario-Based Simulation in This Research: During the evaluation phase, scenario-based simulation plays a clear and practical role. It is the primary instrument for demonstrating end-to-end functionality:

- *Demonstrating end-to-end functionality*: The research team will execute a set of predefined scenarios tailored to the HR and finance departments of SGU. Examples include locating an expiring contract, performing a semantic search for a policy document, and classifying a newly scanned form.
- *Validating operational improvements*: Successful completion of these scenarios provides empirical evidence that the integrated system delivers measurable improvements over SGU's existing fragmented, manual processes.
- *Providing Evidence for RQ3*: The results will contribute to answering Research Question 3 (RQ3) by demonstrating the feasibility and effectiveness of the proposed architecture in a realistic, albeit simulated, operational context.

2.9.2.3 Validation of AI-Powered Features (OCR, Metadata Classification, and Q&A)

To ensure the accuracy, dependability, and trustworthiness of outputs from artificial intelligence (AI), it is essential to validate AI-powered features as they become more embedded in document governance systems. A lack of validation can result in misinformation, misclassification, or reduced explainability, which has a direct impact on user confidence and system adoption (Amershi *et al.*, 2019; Tao, Gao and Wang, 2019).

For an AI-enhanced system, confirming that a feature "*runs*" is not enough. The accuracy and reliability of AI-generated outputs must be explicitly validated to ensure

the system is trustworthy and compliant. Inaccurate AI outputs directly violate the data integrity principles required by ISO standards and undermine user confidence. Therefore, this research includes a specific validation step for the core AI-powered features.

Justification for AI Feature Validation: This validation is a necessary extension of the functional testing process. Rather than simply checking for pass/fail, it quantitatively or qualitatively assesses the quality of the AI outputs.

- *Ensuring Trust and Reliability:* Users will not adopt a system if they cannot trust its outputs. Validating the accuracy of optical character recognition (OCR), classification, and Q&A is fundamental to building this trust.
- *Meeting Governance Requirements:* The integrity of records is a core tenet of ISO 15489. If the AI incorrectly classifies a document or extracts the wrong date, the record's integrity is compromised. This validation step ensures that the AI's performance aligns with these governance requirements.

Application of AI Feature Validation in This Research: The validation process will focus on the technical accuracy and reliability of the three core AI functions. This validation's specific "job" is to:

- *Validate OCR accuracy:* The output of the Google Vision API will be compared to a set of benchmark documents to ensure high accuracy in text conversion.
- *Validate metadata classification accuracy:* The classification and metadata tags generated by Vertex AI will be compared against a manually verified "ground truth" to confirm that documents are categorized correctly according to the defined schema.
- *Validate semantic Q&A relevance:* A human expert will review the answers provided by Gemini AI to a predefined set of questions for contextual correctness and relevance to the source documents.

The purpose of this proof of concept (PoC) is to demonstrate that the AI components operate reliably and produce accurate results consistent with SGU's governance requirements. As previously mentioned, a full-scale human-AI interaction (HAI)

evaluation focusing on aspects such as user trust, cognitive load, and AI explainability is recommended for future research during full implementation.

Chapter 3 will detail the specific accuracy thresholds and validation protocols for each AI feature.

2.10 Overview of Commercial and Open-Source DMS Solutions

Enterprise document management systems (DMS) and content management systems (CMS) have long played a crucial role in helping organizations organize, store, retrieve, and secure digital documents. In knowledge-intensive environments, such as universities, these systems support administrative efficiency, compliance, and institutional memory by facilitating workflows across academic, legal, and operational domains.

A key justification for this Design Science Research project is the finding that existing commercial and open-source document management systems (DMS) are not suitable for SGU's specific needs. This section provides a comparative analysis of popular DMS platforms to illustrate the gap that the proposed system aims to address.

2.10.1 Analysis of Representative DMS Platforms

- **Microsoft SharePoint** is a widely adopted enterprise content and collaboration platform that offers version control, secure access management, metadata tagging, and workflow automation. Its seamless integration with Microsoft 365 tools has made it popular in the education and corporate sectors. However, effective deployment often requires a substantial investment in Microsoft ecosystem expertise and licensing (Rhodes, 2019).
- **Alfresco** is an open-source document management system (DMS) recognized for its flexibility and extensibility. It supports document capture, automated workflows, and fine-grained access control, appealing to organizations seeking vendor independence. However, the open-source edition usually requires substantial technical expertise for customization and maintenance (Sousa *et al.*, 2016).

- ***M-Files*** is a commercial, metadata-driven platform that emphasizes intelligent search, automated classification, and granular access control. While it offers strong usability and AI-assisted features, its licensing costs are comparatively high. Additionally, integration with non-native ecosystems (e.g., Google Workspace) requires custom API development (Asılı and Tanrıover, 2014).
- ***Documentum*** is an enterprise-grade solution developed by OpenText that is particularly strong in compliance-heavy and regulated environments, such as finance, pharmaceuticals, and government. However, its sophisticated workflow, auditing, and security requirements come with high implementation complexity and cost (Singh and Gildhiyal, 2023).
- ***AODocs*** is a cloud-based solution designed to extend Google Workspace with structured document control, compliance workflows, and audit logging. Its native integration with Google Drive makes it attractive for GWS environments; however, its SaaS subscription model introduces recurring per-user costs and a proprietary abstraction layer over Drive that may limit flexibility ('Google Workspace', 2025).

Other specialized solutions, such as OnBase by Hyland and OpenKM, are used in higher education for admissions, accreditation, and faculty management. However, budget constraints, infrastructure readiness, and change management challenges limit their adoption in Southeast Asia (Hidayat and Sensuse, 2022).

Although there are many powerful DMS solutions, they typically fall into categories that pose significant barriers to adoption for an institution like SGU:

- ***Enterprise content platforms (e.g., Microsoft SharePoint and Documentum):*** These platforms are powerful, but often expensive and complex to implement. They would also require SGU to manage an entirely separate technology stack from its existing Google Workspace ecosystem.
- ***Open-source solutions (e.g., Alfresco):*** While these platforms are flexible and low-cost initially, they require significant in-house technical expertise for customization, deployment, and ongoing maintenance, which is a major constraint.

- **Google-native add-ons (e.g., AODocs):** While these solutions offer excellent integration with Google Workspace, they introduce recurring per-user SaaS licensing costs and proprietary constraints that limit SGU's autonomy and long-term flexibility.

The following table provides a comparative overview, highlighting the trade-offs between these platforms in the context of SGU's needs.

Table 2.8 Comparative Overview of Prominent DMS Platforms

Platform	Key Features	Deployment Model	Complexity	Cost Implications	Relative Fit for SGU
Microsoft SharePoint	Versioning, metadata, permissions, workflows, co-authoring	Cloud / On-premise	High: requires Microsoft ecosystem expertise	High: licensing, training, potential custom dev	Low – Not natively integrated, high cost, and high learning curve for SGU staff
Alfresco	Document capture, workflow, open-source, strong access control	Cloud / On-premise	Medium–High: requires Java + Linux skills	Low–Medium: free core, paid enterprise tier	Low–Medium – Flexible but demands high technical skills SGU may not have in-house
M-Files	Metadata-driven search, version control, AI tagging, e-signatures	Cloud / Hybrid	Medium: easier setup, but some learning curve	High: commercial licensing, limited self-host options	Medium – Good AI features but costly
Documentum	Full document lifecycle, regulatory compliance, audit trail	On-premise / Private Cloud	Very High: extensive setup & IT staff needed	Very High: infrastructure-heavy, costly license	Low – Overkill for SGU's scale, high complexity
AODocs	Document control on GWS, workflow automation, compliance logging	Google Workspace native	Low–Medium: simple setup on GWS	Medium: SaaS pricing, but leverages GWS infrastructure	Medium–High – Best fit among commercial tools but costly and limited flexibility

2.10.2 Justification for the Proposed System Over Commercial Alternatives

The analysis reveals that, for SGU, adopting an off-the-shelf DMS would be impractical due to high recurring costs, implementation complexity, and failure to leverage the university's existing Google Workspace investment (detail comparison of cost presented in Appendix B).

Therefore, the proposed AI-enhanced system, which is built entirely within SGU's existing GWS-E+ environment, is the most viable solution. This approach directly addresses the identified gaps by:

- **Minimizing costs:** Leveraging existing licenses and infrastructure avoids the need for expensive new software procurement.
- **Reducing complexity:** It builds upon familiar tools (Drive, Sheets, and Forms), significantly reducing the learning curve and change management burden for staff.
- **Maximizing existing investments:** It enhances, rather than replaces, SGU's current technology stack to ensure a unified and integrated user experience.
- **Maintaining Institutional Autonomy:** It avoids vendor lock-in, allowing SGU to retain full control over its data, governance, and future system development.

In conclusion, designing and building a custom PoC is a necessity, not just a preference, driven by a clear market gap for a powerful, affordable, fully integrated solution that aligns with SGU's technological and operational context.

2.11 Previous Studies and Gap Analysis

The integration of artificial intelligence (AI) into document and contract governance in higher education institutions (HEIs) has been examined from various disciplinary viewpoints, including computer science, information governance, and educational technology. This section provides a critical review of previous studies across five interrelated themes:

- (1) AI applications in document and contract governance
- (2) Enterprise architecture frameworks in HEIs

- (3) IT governance standards and compliance frameworks
- (4) Design Science Research (DSR) application in AI-enabled system prototyping
- (5) The role of Google Workspace and AI in educational environments

Rather than functioning as a catalogue of isolated works, this review takes an integrated, critical approach, identifying technical and organizational gaps in the existing literature. Synthesizing insights from these interconnected domains, the analysis reveals this research's unique contribution: a proof-of-concept (PoC) system leveraging AI within a standards-aligned, enterprise architecture-driven framework to address real-world governance challenges in resource-constrained HEI contexts. The section concludes with a targeted gap analysis demonstrating how the proposed system advances current knowledge and practice.

2.11.1 AI in Document and Contract Governance

Although advances in artificial intelligence (AI) for document and contract governance show promise, they remain limited and largely confined to standard workflows. A recent systematic literature review by Sumarsono and Wibowo (2025) examined publications from 2014 to 2023 and found that machine learning applications in record classification primarily use traditional supervised algorithms, such as Naïve Bayes, decision trees, and support vector machines. Their analysis also highlights a geographic bias toward studies from the Global North and a lack of adoption of deep learning or large language model (LLM) techniques (Sumarsono and Wibowo, 2025).

Complementing this empirical perspective, Souheir and Boukerzaza (2025) conduct a theoretical exploration of AI's transformative potential in higher education institutions (HEIs). They highlight how AI can streamline administrative document management and improve lifecycle control. However, their analysis also highlights critical institutional challenges, particularly regarding governance readiness, ethical considerations, and transparency in automated systems (Souheir and Boukerzaza, 2025).

Sumarsono and Wibowo provide concrete, empirical observations that reveal the reasons behind the slow adoption of advanced AI techniques. Souheir and Boukerzaza provide a convincing rationale for AI deployment within higher education institutions (HEIs). However, both studies fall short of addressing the specific and complex domain of contract governance, including contract lifecycle management, renewal alerts, and metadata-driven compliance. Importantly, neither study incorporates an architecture aligned with governance standards such as ISO 15489 or COBIT, nor do they demonstrate operational deployment in a real institutional setting.

This research addresses this gap by creating a proof of concept (PoC) that focuses specifically on AI-enhanced document and contract governance within SGU. The system advances beyond conventional machine learning (ML) by leveraging:

- LLM-powered semantic Q&A using Google Gemini for intuitive queries across contract documents;
- OCR-based archival digitization via the Google Vision API;
- AI-generated metadata classification through Vertex AI, structured according to ISO 23081 standards; and
- Automated contract alerts integrated with Google Calendar for proactive compliance.

These components are integrated within a TOGAF ADM Phases B–D enterprise architecture to ensure alignment with the institution’s business and data requirements. The architecture is also grounded in the ISO 15489 and COBIT 2019 frameworks for governance and reliability.

By demonstrating AI-driven functionalities and architecture-compliant deployment in a live higher education institution (HEI) environment, this study materially extends the limitations identified in existing literature, especially in Global South contexts, where AI innovation and governance capacity are critical areas of development. The following table summarizes the strengths, limitations, and research gaps identified in the reviewed studies of this thematic area.

Table 2.9 Summary of Previous Studies on AI in Document & Contract Governance

Study & Year	Strengths	Limitations	Research Gap Addressed by This Study
Sumarsono & Wibowo (2025)	Systematic review with broad coverage (2014–2023); identifies common ML methods in record classification	Limited to traditional ML; no LLM adoption; mostly Global North studies	Introduces LLM-driven semantic Q&A, OCR, and AI classification in HEI contract governance
Souheir & Boukerzaza (2025)	Theoretical insights on AI adoption in HEIs; considers governance readiness and ethics	No empirical deployment; lacks standards-based architecture	Implements standards-aligned (ISO, COBIT) PoC in a live HEI environment

2.11.2 Enterprise Architecture in Higher Education Institutions (HEIs)

Enterprise architecture (EA) has been widely recognized as a strategic enabler for aligning technology, data, and organizational processes in higher education institutions. In complex institutional settings, such as universities, where academic, administrative, and governance functions often operate independently, EA provides a structured approach to achieving system integration, strategic alignment, and operational efficiency. Among the available EA methodologies, the TOGAF Architecture Development Method (ADM) is the dominant framework. It is valued for its comprehensive approach to business, data, application, and technology architectures.

Empirical evidence demonstrates the potential and limitations of EA implementation in higher education institutions (HEIs). Nama, Forda, and Kurniawan (2017) describe a TOGAF-driven initiative at the University of Lampung that successfully mapped business processes and identified integrated systems to replace fragmented operations. Their work illustrates EA's capacity to provide a coherent blueprint for system planning (Nama, Tristiyanto and Kurniawan, 2017). However, the study's scope is limited to conceptual integration. There is no assessment of the performance of the proposed architecture when implemented, nor consideration of governance or compliance frameworks that could ensure sustainability and accountability.

A similar pattern emerges in the work of Febrianto, Fajrillah, and Febriyani (2024), who used TOGAF ADM 9.2 to develop an enterprise architecture (EA) blueprint for a foundation in education. This study stands out for explicitly including cybersecurity

maturity as a design consideration and for aligning IT transformation with risk management priorities (Febrianto, Fajrillah and Febriyani, 2024). However, the study is still a high-level design exercise. Its lack of empirical validation raises questions about the practical efficacy of such architectures in daily operations, particularly regarding document governance and AI integration.

A broader perspective is provided by Alamri, Abdullah, and Albar (2018), who offer a conceptual analysis of EA adoption in higher education institutions (HEIs), positioning EA as a driver of institutional effectiveness through better decision-making and performance monitoring. While their SWOT-based approach highlights important adoption challenges, such as governance capacity, stakeholder engagement, and tool selection, the absence of an operational prototype or empirical results limits the study's contribution to actionable guidance (Alamri, Abdullah and Albar, 2019).

A common theme emerges across these works: Enterprise architecture (EA) in higher education is usually discussed at the design or strategic level, with little progress toward operationalization and measurable impact. None of the reviewed studies explore how EA could be directly integrated with AI-powered document governance tools or address compliance with international records management and IT governance standards. This gap is particularly notable as universities increasingly seek to integrate systems and embed intelligence and compliance into their digital infrastructures.

This study bridges this gap by implementing TOGAF ADM Phases B–D within a live higher education institution (HEI) environment and embedding AI-driven functionalities, such as optical character recognition (OCR), automated metadata classification, and semantic question-and-answer (Q&A) requirement, directly into the enterprise architecture. Furthermore, by aligning the system with ISO 15489 for records management, ISO 23081 for metadata governance, and COBIT 2019 for IT governance, this study advances EA research from blueprinting to a standards-aligned, AI-enabled, empirically validated proof of concept. It demonstrates the architectural feasibility of integrating AI into document and contract governance in HEIs and provides an

evidence-based model for institutions transitioning from fragmented, manual processes to intelligent, compliant workflows.

The comparative synthesis of these studies is presented in table 2.11, which distils their respective strengths, limitations, and the specific research gap addressed by this thesis.

Table 2.10 Summary of Previous Studies on Enterprise Architecture in HEIs

Study	Strengths	Limitations	Research Gap Addressed by This Study
Nama, Forda & Kurniawan (2017)	Demonstrated how TOGAF can map HEI business processes and highlight integration opportunities.	Limited to conceptual planning; no empirical system validation; lacks compliance framework integration.	Moves from conceptual EA design to a live, AI-enabled PoC tested within an HEI; embeds ISO and COBIT compliance.
Febrianto, Fajrillah & Febriyani (2024)	Incorporates cybersecurity maturity into EA blueprint; aligns with risk management principles.	No operational prototype; limited focus on document governance; lacks AI-driven process integration.	Integrates AI-based document governance directly into EA, operationalised in a working prototype.
Alamri, Abdullah & Albar (2018)	Identifies strategic benefits of EA adoption in HEIs and maps adoption challenges via SWOT.	No technical implementation; lacks integration with intelligent systems; does not address compliance standards.	Demonstrates standards-aligned EA with operational AI tools for document and contract governance in HEIs.

2.11.3 IT Governance Standards in Higher Education Institutions (HEIs)

In higher education institutions (HEIs), effective IT governance is a structural requirement that aligns IT initiatives with academic, administrative, and compliance goals, not merely a matter of technical control. Although frameworks such as COBIT 2019, ISO 15489, and ISO 23081 provide well-defined processes for governance, records management, and metadata control, their adoption in HEIs remains uneven. Although the literature shows growing recognition of their value, they are only minimally applied in AI-enhanced document governance contexts.

Utomo et al. (2022) conducted a case study in which they applied COBIT 2019 to evaluate IT governance maturity in a higher education environment. The study used COBIT's process assessment model to identify strengths in strategic alignment and resource optimization while revealing weaknesses in security governance and change

management (Utomo *et al.*, 2022). The authors demonstrated how COBIT's structured domains, such as Align, Plan, and Organize (APO) and Deliver, Service, and Support (DSS), could guide policy reform in HEIs. However, the application of these models remained largely process-audit oriented, stopping short of embedding governance controls into day-to-day operational systems. Consequently, the study's ability to demonstrate real-time governance enforcement in areas such as automated document workflows or AI decision-making was limited.

Similarly, Fitriyani and Muhammad (2025) used COBIT 2019 to evaluate the maturity of ICT governance in an Indonesian university setting. Using a quantitative maturity model, they determined that domains such as APO04 (Managed Innovation) and DSS01 (Managed Operations) had reached Level 3 (Established) maturity (Fitriyani and Muhammad, 2025). While this indicates stable governance practices, the study also revealed an absence of proactive risk management and weak integration between governance policies and technological innovations. While the study validated COBIT's adaptability in higher education institutions (HEIs), it, like Utomo *et al.*, remained disconnected from automation and artificial intelligence (AI), leaving unanswered questions on how governance could be embedded in intelligent document or contract systems.

From a records management perspective, Findlay (2018) examined the evolving role of ISO 15489 in ensuring the authenticity, reliability, and usability of institutional records. The study traced the standard's historical development and its emphasis on compliance and accountability, offering valuable insight into metadata control and lifecycle management (Findlay, 2018). While Findlay acknowledged the growing digitization of records, the study did not address AI-assisted metadata extraction or automated compliance monitoring. This creates a gap between theoretical governance principles and modern, AI-driven document systems.

Together, these works confirm the relevance and adaptability of IT governance and records management standards in higher education institutions (HEIs). However, they primarily focus on assessment and policy, evaluating governance maturity and

clarifying theoretical standards, without translating these into operational systems that integrate AI for governance enforcement. None of the studies address how COBIT 2019 controls, ISO 15489 compliance rules, or ISO 23081 metadata frameworks can be embedded in an operational AI-powered system for governing documents and contracts that operates under a defined enterprise architecture.

This study addresses these gaps showing in the following table 2.12 by embedding COBIT 2019's governance principles and ISO 15489 / ISO 23081 metadata rules into an **operational Proof-of-Concept (PoC)** built on **Google Workspace for Education**. AI-powered features—such as OCR-based digitization, AI-driven metadata extraction, semantic Q&A, and automated contract reminders—are governed, audited, and traceable in line with these standards. This integration demonstrates how governance frameworks can move beyond assessment to **active, automated enforcement**, representing a significant step forward in practical IT governance for HEIs.

Table 2.11 Comparison of IT Governance Standart Studies

Study	Strengths	Limitations	Gap Addressed in This Study
Utomo <i>et al.</i> (2022)	Applied COBIT 2019 maturity assessment in HEI; identified governance domain gaps	No operational embedding of governance controls in live systems	Integrates COBIT controls into an AI-enhanced, operational document governance PoC
Fitriyani & Muhammad (2025)	Quantitative evaluation of governance maturity; identified innovation and operational strengths	Lack of linkage between governance policies and AI/automation	Operationalises governance policies with AI-driven document workflows and metadata management
Findlay (2018)	Comprehensive theoretical update on ISO 15489 for record authenticity and lifecycle management	No application in AI-enabled or automated systems	Embeds ISO standards directly into AI-enabled document and contract compliance processes

2.11.4 Design Science Research (DSR) & AI Prototyping

Design science research (DSR) has been established as a methodological cornerstone for developing and evaluating innovative artifacts that address real-world problems. Peffers et al. (2007) first articulated this structured process, which encompasses problem identification, objective definition, design and development, demonstration, evaluation, and communication. This model balances rigor and relevance, ensuring that

research outcomes are theoretically grounded and practically applicable (Pefferers *et al.*, 2007). However, the original framework predates the rise of AI-driven systems and does not explicitly address the complexities of integrating intelligent components into the artifact lifecycle.

Recent scholarship has begun to address this gap. For example, Gau *et al.* (2025) expanded the DSR methodology to incorporate AI-augmented design cycles. They emphasized how machine learning, natural language processing, and other intelligent technologies can be embedded into the artifact itself and the design process (Gau *et al.*, 2025). They demonstrate that AI can enhance ideation, accelerate prototyping, and improve evaluation precision but can also introduce challenges regarding transparency, explainability, and bias mitigation. However, their work remains largely conceptual and lacks applied case studies within higher education institutions (HEIs) or compliance-intensive environments, such as document governance.

From a more practical standpoint, Truss and Schmitt (2024) examined the incorporation of no-code and AutoML platforms into DSR prototyping stages. They argue that democratizing AI development by enabling non-technical stakeholders to participate in artifact design can improve user acceptance and institutional adoption (Truss and Schmitt, 2024). However, their study is limited to theoretical frameworks and controlled laboratory scenarios without addressing enterprise-scale integration or governance requirements.

Together, these studies illustrate the evolving landscape of DSR in the AI era. Pefferers *et al.* provide the foundational methodology, Gau *et al.* extend its conceptual boundaries to accommodate AI, and Truss and Schmitt explore inclusive tools for rapid prototyping. However, none of these studies apply these approaches to a real-world, governance-aligned, AI-enhanced document management system in a higher education institution (HEI) context, particularly one that must operate within the architectural constraints of the Open Group Architecture Framework (TOGAF) and comply with standards such as ISO 15489, ISO 23081, and COBIT.

This research addresses this omission by embedding AI functionalities, such as OCR-driven digitization, semantic Q&A, and automated metadata classification, within a proof-of-concept (PoC) system developed through a DSR approach. Unlike prior studies, this work situates the artifact within an enterprise architecture framework and validates it against technical performance and governance compliance criteria. Table 2.13 below summarizes the key strengths, limitations, and identified research gaps from the reviewed literature.

Table 2.12 Summary of DSR & AI Prototyping Studies

Study	Strengths	Limitations	Gap Addressed in This Study
Peppers et al. (2007)	Established, widely adopted DSR methodology; systematic steps from design to evaluation.	Pre-dates AI focus; no guidance for intelligent system integration.	Applies DSR rigor to an AI-enabled governance prototype in HEI context.
vom Brocke et al. (2020)	Extends DSR for AI integration; considers ideation, prototyping, and evaluation with AI.	Conceptual; lacks applied HEI or compliance-oriented case studies.	Demonstrates AI-augmented DSR iteration within governance and enterprise architecture context.
Truss & Schmitt (2024)	Advocates no-code AI prototyping; improves inclusivity and stakeholder engagement.	Theoretical; no enterprise-scale deployment or governance alignment.	Implements inclusive AI prototyping within a compliance-bound, institution-wide governance system.

2.11.5 Google Workspace & AI in Higher Education Institutions (HEIs)

The growing use of Google Workspace in higher education institutions (HEIs) has transformed administrative and pedagogical practices. Beyond its core productivity tools, the recent integration of AI, especially with the introduction of Gemini, promises to redefine document governance, collaboration, and adaptive learning within educational contexts.

Emilzoli et al. (2025) conducted a study investigating student perceptions of Google Workspace's effectiveness in collaborative learning at an Indonesian university. Using the Technology Acceptance Model (TAM), the researchers found that students perceived the tools as easy to use and useful for teamwork and productivity (Emilzoli

et al., 2025). However, this study focuses on pedagogical outcomes and lacks exploration of institutional governance, document control, and AI requirement.

In terms of administration, Sismanto, Cikusin, and Mistar (2024) conducted a qualitative analysis of the challenges that educational leaders face when implementing Google Workspace for Education in Indonesia. The researchers highlighted various barriers, such as resistance to change, infrastructure limitations, and the need for leadership support, and they proposed practical strategies, including enhanced training, infrastructure readiness, and policy alignment (Sismanto, Cikusin and Mistar, 2024). While valuable for understanding institutional adoption hurdles, this study did not address how Google Workspace could integrate AI-based systems to support compliance or document governance needs.

The rapidly evolving landscape of AI in education also warrants attention. Google's multi-billion-dollar investment in AI tools, including offering advanced requirement such as Gemini for Education at no additional cost, demonstrates institutional momentum toward integrating AI into workspace ecosystems (*Gemini AI is now for students: Here is what you need to know*, 2025). Yet, academic analyses of how these AI integrations impact institutional governance, workflow automation, or document control remain scarce.

These studies collectively underscore the value of Google Workspace as a collaborative platform and highlight real-world adoption challenges. However, none of them explore the intersection of AI-enhanced governance within Workspace environments. A critical gap remains in our understanding of how AI tools like Gemini can be embedded to enforce document standards, automate metadata extraction, and align with governance frameworks in higher education institutions (HEIs).

This thesis addresses this gap by developing a proof of concept (PoC) that integrates AI requirement, including optical character recognition (OCR), metadata classification, semantic question-and-answer (Q&A), and contract alerts, directly into Workspace-based workflows. These features operate within an enterprise architecture framework

and comply with governance standards, including ISO 15489, ISO 23081, and COBIT. This approach transforms Google Workspace from a passive collaborative tool into an intelligent, compliant system for document and contract governance. The table below summarizes the strengths, limitations, and research gaps of existing studies on Google Workspace and AI in higher education. This sets the stage for how the current literature is being innovatively extended through this research.

Table 2.13 Summary of Google Workspace & AI in Higher Education Studies

Study	Strengths	Limitations	Gap Addressed in This Study
Emilzoli <i>et al.</i> (2025)	Empirical TAM-based evaluation of student perceptions; high adoption intent for Workspace tools.	Focused on learning outcomes; no governance or AI-focused analysis.	Embeds AI-driven governance tools into Workspace workflows under standards-compliant framework.
Sismanto <i>et al.</i> (2024)	Identifies leadership and infrastructure challenges for institutional Workspace adoption.	Does not explore AI integration or compliance-oriented functionality.	Addresses institutional barriers while integrating AI-enhanced document governance within Workspace.
Google AI for Education initiative (2025)	Demonstrates large-scale AI deployment via Gemini tools within Education editions of Workspace.	Mostly technological rollout; lacks academic investigation of governance impacts.	Implements governance-aligned AI features within Google Workspace workflows for document control.

2.12 Designing an Integrated Framework for Research and Governance

The preceding review established the strengths of several key frameworks and methodologies. However, the literature reveals that no single framework is sufficient for addressing the complex, multilayered challenge of designing and implementing an AI-enhanced governance system in higher education. A purely architectural approach, such as TOGAF, lacks specific governance controls. A governance framework like COBIT is not a design methodology. DSR, a research paradigm, is a high-level process that requires a more detailed engine to drive its cycles.

Therefore, one of the central contributions of this research is the design of a new, integrated framework that combines these components into a coherent, practical model. This section explains the rationale behind the design of this unique framework and details how and why the standard models were modified and combined.

2.12.1 The Design of the Modified Governance Framework

The proposed governance framework is a synthesis designed to leverage the complementary strengths of TOGAF, ISO, and COBIT. Rather than a simple layering, it is a deliberate integration in which each component plays a specific role:

- **The "how" (the process): TOGAF's ADM.** TOGAF's ADM was selected to serve as the foundational process backbone. It provides a structured, step-by-step methodology for transitioning from business requirements to a final technical architecture.
- **The "what" (the rules): ISO 15489 and 23081.** These ISO standards are embedded within the TOGAF process as the definitive set of rules. These standards provide specific, internationally recognized requirements for reliable records and well-structured metadata. They inform design decisions made in TOGAF's business and data architecture phases.
- **The "control" (the governance layer): COBIT 2019.** The COBIT framework is applied as the overarching governance and control layer. Its risk management, security, and compliance objectives provide the criteria by which the architectural design is validated. This ensures that the final system is functional, auditable, and secure.
- **The "engine" (The Automation): AI Services.** Finally, artificial intelligence is integrated as the automation engine. This technology allows the rules (from ISO) and controls (from COBIT) to be efficiently executed within the TOGAF-provided structure.

2.12.2 Adapting the DSR Methodology for a Complex Project

Similarly, adaptation of the research methodology was necessary. Although Hevner's three-cycle DSR model is a powerful conceptual guide (please refer to Section 2.8.1 and Figure 2.5), it is not a prescriptive, step-by-step process. While it specifies what to balance (rigor, relevance, and design), it does not provide guidance on how to manage a complex project that integrates multiple large-scale enterprise frameworks, such as TOGAF and COBIT. Directly applying the high-level model would lack the necessary structure and detail to guide a project of this nature.

Therefore, to operationalize Hevner's abstract model in this context, this research makes the following design choices to adapt it:

1. **The TOGAF ADM is used as the engine for the design cycle:** The research uses the TOGAF Architecture Development Method (ADM) as the structured engine to drive architectural activities within the central design cycle. This provides a much more detailed and rigorous process for moving from requirements to a final architecture than the generic DSR model alone.
2. **The Agile SDLC as the Engine for Prototyping:** Within the broader design cycle, the practical, hands-on development of the prototype is managed using an iterative agile SDLC. This involves organizing the work into three distinct prototyping cycles, which allows for the systematic and incremental construction of the artifact.
3. **Formalizing the Inputs for the Rigor Cycle:** The research uses ISO and COBIT standards as the primary formal inputs for the Rigor Cycle. This ensures that the "*knowledge base*" is a concrete set of established best practices that directly inform and constrain the design at every step, rather than an abstract concept.

These modifications demonstrate a practical, repeatable method for applying the DSR paradigm to complex, real-world enterprise IT challenges. This adapted methodology is formally presented and executed in Chapter 3.