

Enterprise-Wide Maturity Model for Information Security Risk by Aligning ISO 27001 Controls with Strategic Governance.

Student Name: Md Al Amin Sarkar Reday

Student ID: 2406207

Module Name : Research Methods and Professional Development

Module Code: ACFA7004

Table of Content

Introduction.....	3
Context and Background.....	3
Research Problem.....	4
Research Aim and Objectives.....	4
Significance of the Research.....	5
Literature Review.....	7
Research Design and Methodology.....	10
Research Design.....	10
Research Methods and Materials.....	10
Expected Outcomes.....	13
Timeline (12-Week Schedule).....	14
Conclusion.....	16
References.....	17

Introduction

Context and Background

In the digital age, information security has moved far past its traditional technical boundaries and today is a component of organisational resilience, strategic governance and organisational competitive advantage. The growing frequency, sophistication, and impact of cyber threats, ranging from ransomware attacks to crippling critical infrastructure to nation-state espionage targeting intellectual property, have propelled risk management into the top of executive agendas [1]. Concurrently, a web of complex regulatory requirements, including the General Data Protection Regulation (GDPR), the Network and Information Systems (NIS) Directive, and sector-specific regulations, has created very stringent compliance requirements, making security a legal and fiduciary requirement rather than a best practice. In this turbulent environment organisations are forced to move away from ad-hoc security measures and towards systematic and evidence-based approaches to secure their information assets.

The ISO/IEC 27000 family of standards have become the globally recognised standard for the establishment, implementation, maintenance and continued improvement of an Information Security Management System (ISMS). Specifically, while ISO/CEI 27001 is a requirements framework, its supporting standard, ISO/CEI 27002, is a rich catalogue of 93 security controls grouped in Annex A by 4 themes: organisational, people, physical and technological [1]. These controls, from access control policies to incident management procedures, provide a foundation and holistic set of goals, against which an organisation can measure its security posture. Certification against ISO 27001 shows a commitment to international best practices and an approach to managing information risk to stakeholders.

However, attaining and retaining certification to the ISO 27001 standard, whilst important, can often be a binary state: an organisation, at a point in time, is either compliant or non-compliant with the requirements of the standard. This poses an important limitation. Compliance does not necessarily mean maturity, robustness, or effectiveness. Two organisations with valid ISO 27001 certificates may have widely divergent security postures; one might have implemented controls at a bare minimum, checklist type level while the other will have deeply integrated them into its business processes, with sophisticated monitoring and continuous improvement mechanisms. The standard gives the what--the control objectives--but has little prescriptive information on the how well these controls are implemented, managed, and evolved [2]. This disparity between compliance and capability places senior management and boards at a loss for words. They do not have a clear, quantifiable and longitudinal measure of whether they are developing a mature security programme against industry peers or best practice. Are our security investments improving measurably overtime? We must ask: where should we focus resources so as to get the greatest risk reduction?

Research Problem

Despite the ubiquity of adopting ISO 27001 as a compliance and governance tool, many organisations do not understand how to translate their information security risk assessment activities into a consistent, measurable and strategic score of maturity. Rather than simply a question of compliance, existing approaches for assessing security posture are often manual, fragmented, and highly subjective. Assessments are often based on the skill and opinion of separate auditors or consultants, which result in inconsistencies between different assessors and also over time. The process tends to be document-centric in which policies and procedures are reviewed, and less objective measurement of operational effectiveness or integration into business workflows [2].

Furthermore, most of the existing maturity models in information security are descriptive, rather than operational. They provide generic characteristics for each maturity level (e.g. "At Level 3, processes are documented and standardised") but do not give much granular advice how to map the implementation quality of specific ISO 27001 controls to these levels. This failure to have an exact mechanism to map leads to a number of critical gaps. First, it creates an inconsistency gap: without a standardised scoring rubric maturity assessments are not reproducible or comparable between different business units or organisations. Second, it causes a comparability gap: management cannot compare its own level of maturity with industry averages or best in class peers on a common scale based on a universal standard. Third, it fuels an unending improvement gap: the lack of transparency in the relationship between specific areas of control deficiencies and the overall score on maturity makes it hard to make targeted, prioritised roadmaps for improvement. Investments are made on perceived risk or on the audit findings instead of a real plan to reach the next maturity level.

Research Aim and Objectives

To develop and theoretically assess a maturity-based information security risk assessment framework, based on control objectives of ISO 27001, to allow organisations to meet information security posture through systematic risk assessment, comparison and improvement.

To attain the said aim, following specific objectives have been formulated:

- To critically review and synthesise existing information security risk assessment methods and maturity models that are aligned with the ISO 27000 family of standards.
- To identify the conceptual gaps and the practical limitations in the current maturity-based assessment approaches as presented in the academic and practitioner literature.
- For the conceptual maturity framework to incorporate both of the following: Inclusion of the control objectives of ISO 27001 Annex A. A structured and multi-dimensional scoring mechanism for deriving reproducible maturity levels.

- To provide evidence of the application of proposed framework by conceptual evaluation to illustrate how the framework produces a consistent maturity score and prioritised recommendations for improvement.
- To be able to draw guidelines for the theoretical adoption, continuous monitoring and future enhancement of the proposed framework.

These objectives will be pursued in a desk-based, conceptual research methodology that addresses the following research questions:

- RQ1: What are the key characteristics, strengths and limitations of existing ISO 27001 aligned information security risk assessment and maturity models as identified in the literature?
- RQ2: What are the basic design principles needed to create an operational maturity framework for systematically measuring the quality of implementation of ISO 27001 control objectives?
- RQ3: How to integrate a structured scoring mechanism conceptually with ISO 27001's Annex A in order to create a reproducible and comparable security maturity score?
- RQ4: How does the proposed framework fare in addressing possibilities of conceptual evaluation such as inconsistencies, lack of comparability and poor support for continuous improvement of existing approaches?

Significance of the Research

This research is important, not only to the academic, but also to the professional community. For academia, this is a contribution to the growing literature on information security governance as it is proposing a new synthesis of the compliance and maturity paradigms. It provides for a detailed conceptual model to operationalise the abstract concepts of maturity in the concrete context of the leading information security standard in the world. The research will have a critical engagement with and extension of existing theories on security metrics, risk quantification and organisational capability development[20].

The implications for practical applications and potential applications are very big. For organisations, the proposed framework is a powerful tool to manage strategic security. It can help achieve the path from being a compliance static ISO 27001 to being a maturity dynamic dashboard. Chief Information Security Officers (CISOs) and risk managers could use it as a method of communicating security posture to the board in a language that is clearly communicated and metric driven and used to justify budgets and strategic initiatives. It provides for the benchmarking of an objective nature to be compared with sectors in industry to encourage a culture of continually and measurably improving[17]. For auditors and consultants, the framework provides them a standardised, repeatable methodology for assessments, which makes the assessments more consistent, credible and of higher quality. For regulators and industry

bodies it could tell us what more nuanced, maturity-based regulatory expectations/benchmarks for a sector might look like. Ultimately, by assisting organisations to better measure and manage their security maturity, this research is part of this wider ambition to make the system as cyber resilient as possible in the face of increasing cyber threats.

Literature Review

Introduction to the Literature Review

The purpose of this literature review is to critically assess the existing information on information security risk assessment, maturity models and at the intersection of ISO / IEC 27001 standard. It is aimed at identifying the dominating themes, assessing the contribution of key studies and highlighting the theoretical and practical gaps addressed by the present research. The scope covers academic literature and relevant industry frameworks of the last ten years, with a specific focus on models that try to measure security posture quantitatively, or that incorporate compliance and capability measurement. This review is presented thematically, and moves from the basic standards to generic maturity models and then to security maturity frameworks and, in the end, hybrid approaches to provide information to guide the design of the proposed framework.

ISO / IEC 27001 as the Basic Compliance Framework

ISO/IEC 27001 is recognized world wide as the leading international standard for Information Security Management Systems (ISMS). It provides a risk-based framework in which organisations are required to establish, implement, maintain and constantly upgrade their security posture. The standard's Annex A, supported by ISO/IEC 27002, provides a comprehensive set of control objectives and recommended controls, addressing aspects of technological, procedural and human factors [1]. The main strength of ISO 27001 is the systematic process-oriented approach and the worldwide acceptance of this standard, which is especially helpful for the external certification and to show due diligence [3]. However, an important criticism in the literature has concerned its limitations as regards performance measurement. The standard provides only minimal guidance as to how well they should be implemented or how to measure their effectiveness over time, and we are being left with a potential "checkbox compliance" culture where the letter of the standard is met but little security improvement takes place [4].

Evolution and Use of Capability Maturity Models

Capability Maturity Models (CMMs), originally created for software engineering, define an ordered way of process improvement through defined maturity levels, usually from Initial (ad-hoc) to Optimizing (continuously improving) [5]. The fundamental value proposition for a maturity model is that it can provide a staged, measurable roadmap for incremental improvement, allowing all of the emphasis to be taken off one-time project completion and instead placed on sustained organizational capability. These models have been adapted successfully to various areas, such as project management and service management, showing that they are useful for transposing qualitative attributes of processes into quantifiable maturity levels [6]. The generic architecture of a maturity model consists of defined process areas, capability

levels, and assessment methods which form a combined template that may be specialized into various disciplines such as information security.

Maturity Models for Information Security

In response to the need for better security governance, a number of maturity models specific to cybersecurity have been developed. Models such as Cybersecurity Capability Maturity Model (C2M2) and Security Maturity Model in the NIT Cybersecurity Framework (CSF) provide high-level roadmaps on how to enhance an organization's cyber defense capabilities [7]. These frameworks usually define key domains (e.g. Risk Management, Asset Management) and characterize characteristic practices at each maturity level. Their strength is in supplying strategic direction and communication with the senior management about the cybersecurity posture. However there is a common weakness in the literature: these models can be essentially descriptive and not granular. They do not offer an exact and unambiguous translation to the particular control goals required by broadly adopted standards such as ISO 27001, and thus they create difficulties for organisations to directly map their efforts towards compliance with a maturity score [8].

Existing Hybrid Approaches: The Compliance vs. Maturity

One of the ways of recognizing that disconnect has been various efforts by academics and practitioners to develop hybrid approaches to combine compliance models and maturity concepts. Some researchers have suggested that the controls of ISO 27001 should be mapped to the domains of the NIST CSF for a more comprehensive evaluation tool [9]. Other studies have created maturity assessment questionnaires based on ISO 27002, which assign qualitative maturity levels (such as non-existent, initial, repeatable, defined, managed, optimized) to groups of controls [10]. These approaches are important steps towards integration. They confirm, and give initial methods for making more subtle assessments than pure compliance audits, of interest in unifying these paradigms.

Shortfalls in the Technical Implementation and Scoring Mechanisms

A critical analysis of these hybrid approaches shows a wide gap in operationalization, especially with respect to the scoring mechanism. Many models that have been suggested are still of the high-level, qualitative kind. The process of reaching a level of maturity often is described in very general terms, relying heavily upon assessor judgement, rather than some reproducible, algorithmic scoring system [11]. There is no detailed literature available on how to build a weighted, multi-attribute scoring mechanism that can combine the status of implementation of dozens of individual ISO 27001 controls into a single, comparable maturity index. Furthermore, few models explicitly address how to treat partial compliance or different types of control implementation effectiveness in a quantifiable way, which is crucial to the generation of precise improvement roadmaps for action [12].

Theoretical and Technical Requirements of Framework Design

The design of an operational maturity framework must have strong theoretical and technical foundations. From a theoretical perspective, the framework must be anchored in well-established principles of measurement theory and risk management in order to assure that the products of the framework are valid and meaningful [13]. Technically, it is necessary to define clear parts of the architecture: a set of controls (based on ISO 27001 Annex A), a scale of maturity (for example, a 5-level scale), assessment indicators for the controls in each level, and an aggregation formula. The literature on multi-criteria decision analysis (MCDA) provides useful methods, such as the analytic hierarchy process (AHP) for prioritizing the relative weight on the various control domains or themes, to reflect their strategic importance for the organization [14]. These technical components are referred to often in isolation and are seldom put together into a coherent, end-to-end framework design in the context of ISO 27001.

Placing the Current Study in the Literature

This research establishes itself right in the gap identified between high-level hybrid models and operational, quantifiable assessment tools. While previous efforts have managed to make the case for combining ISO 27001 and maturity concepts and suggested conceptual mappings, the goal of this research is to take the field forward by creating a detailed conceptual framework with a structured scoring mechanism. It goes beyond explaining that there should be a link, to how it can be systematically carried out to create a repeatable measure. The proposed framework aims to overcome the shortcomings of inconsistency, poor comparability and poor support for continuous improvement by establishing a standardised transparent methodology to translate compliance data into a maturity score.

Literature Gap Summary

The synthesis of the reviewed literature shows that a clear and persistent gap exists. While ISO/IEC 27001 defines core security controls [16] and generic maturity models offer a framework of capability progression, a dearth of a detailed, operational and widely applicable framework that systematically combines the specific control objectives of ISO 27001 Annex A with a structured, quantitative maturity scoring mechanism. Existing hybrid models frequently exist at the conceptual, high-level, or subjective judgement level, and do not deliver the granular, reproducible and algorithmic-driven assessment tool required by organizations supporting strategic security governance[15]. This gap leads to the previously identified key challenges - inconsistent assessments, an inability to benchmark objectively and an inability to develop prioritized, metric driven plans for improvement. This research is intended to fill this exact gap by the development and theoretical assessment of a framework in which the maturity assessment of an ISMS can be operationalized on the basis of its foundational standard.

Research Design and Methodology

Research Design

This study is using a Design Science Research (DSR) paradigm as an overall research design. DSR is fundamentally concerned with the creation and evaluation of innovative artifacts (including models, frameworks, methods, or instantiations) that are intended to solve identified organizational problems [15]. Given that the ultimate goal of this research is to create a new maturity framework (the artifact) to bridge the gap between the ISO 27001 compliance and the measurable security maturity, DSR is the right and rigorous methodological foundation. The process of DSR as formalized by Hevner et al. involves a cycle of problem identification, artifact design, demonstration, evaluation and communication which exactly matches the structure of this proposal [16]. This is theoretical and desk-based work - so the artifact will be a conceptual framework along with its scoring mechanism, not a functional software tool. The research will move forward through the core DSR activities: 1) Problem Identification (taken care of in the Introduction and Literature Review), 2) Artifact Design (Objective 3) 3) Demonstration (Objective 4), and 4) Evaluation (conceptual evaluation within Objective 4). This design is justified as it does not stop at a description of a problem, but actively proposes and appraises a novel solution to a problem, thus fulfilling the requirement for originality and understanding of practical application at Level 7.

Research Methods and Materials

Methods

The research will use a suite of complementary, qualitative methods in the DSR cycle to fulfill their objectives.

Literature Synthesis and Critical Analysis: The method to be used primarily to achieve Objective 1 and Objective 2 will be literature synthesis and critical analysis. A systematic approach will be taken to a literature review, building on the basic literature review. Existing models of maturity (e.g. C2M2, NIST CSF maturity indicators) and those that are aligned to ISO 27001, will be deconstructed to help extract core components, assessment logic, and limitations. This analysis will directly feed in with the design principles for the new framework, which answers RQ1 and RQ2. The synthesis will not just be a summary, but will involve critical comparison and contrast between approaches for solidifying the argument for the proposed design.

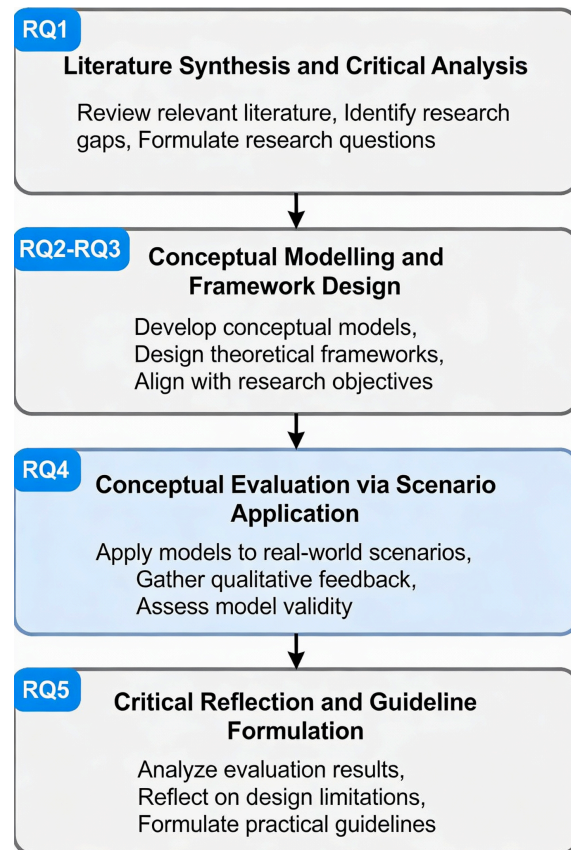
Conceptual Modelling and Framework Design: This is the fundamental approach for Objective 3. Following the principles of DSR, the maturity framework, the artifact, will be designed in an iterative process of conceptual modelling. This includes defining the core constructs of the framework: adapted control set from ISO 27001:2022 Annex A, maturity scale (e.g. a 5 level

scale from Ad-hoc to Optimising) and assessment indicators for each control for each level of maturity. Crucially, during this phase, the structured mechanism of scoring will be designed. Techniques borrowed from multi-criteria decision analysis will be conceptually applied to the development of a transparent scoring algorithm. This algorithm will determine how evidence for each control is mapped to a maturity level, how scores for controls are aggregated within domains (thematic groups of controls) and how a final, overall Organizational Security Maturity Index (OSMI) is calculated. This process is a direct response to RQ3 by determining the mechanism of integration.

Conceptual Evaluation via Scenario Application

To meet Objective 4 and get an initial evaluation as mandated by DSR a conceptual Demonstration or "proof-of-concept" will be done. This is the application of the designed framework in a hypothetical or generic organizational situation. A series of simulated assessment data for a number of ISO 27001 controls will be created. The scoring mechanism of the framework will then be manually applied to this data to generate a maturity profile (both domain-level and overall scores). The result will be analyzed in order to show how the framework works: how a score is obtained, what are weak areas, and, reverse engineering of the scoring, some suggestions of prioritized improvements to be made (e.g. focus on controls in Domain A to advance from Level 2 to Level 3). This evaluation does not address empirical validity but shows utility, internal consistency and addresses RQ4 by showing how the framework addresses the gap like inconsistency and poor support for improvement.

Critical Reflection and Guideline Formulation The last method, which supports Objective 5, is a phase of critical reflection on the designed artifact. Based on insights gained in the design and conceptual evaluation, theoretical guidelines for adoption will be drawn. This includes representing the need for prerequisite for use, a proposed process for conducting an assessment, strategies for incorporating the framework with existing ISMS audit cycle and a model for ongoing monitoring and updating of maturity over time. This reflective method provides the guarantee not only that the research outputs are not an artifact, but also that prescriptive knowledge about their application is included.



Materials

The research materials are all documentary; and conceptual tools, in keeping with the theoretical research study.

Research Data: The prime "data" for this research is extant literature and normal documentation

Data Sources: Scholarly peer-reviewed articles from scholarly databases (IEEE Xplore, ACM Digital Library, ScienceDirect), Official ISO standards (ISO/IEC 27001:2022, ISO/IEC 27002:2022) and well known frameworks from the industry or from government (NIST CSF, C2M2 documentation). These sources will be the raw material for the literature synthesis and as the basic control set for the framework.

Data Collection Method: Retrieval and Analysis of Documents Key search words will be: "information security maturity model", "ISO 27001 maturity", "security metrics", "capability maturity model integration", "risk assessment framework".

Justification: These sources are directly appropriate as being part of the body of knowledge that the research attempts to engage with, extend and synthesize. Academic literature provides us with critical analyses and prior models and the ISO standards provide us with the authoritative and internationally recognized control objectives which are the non-negotiable basis of the artifact.

Ethical Considerations: Since this research is based on the use of publicly available documents and published standards, there are no significant ethical considerations regarding data privacy, consent, or collection. All of the sources will be properly cited in order to ensure academic integrity and prevent plagiarism.

Software and Analytical Tools: Considering the conceptual nature of the study, no certain software for data analysis is required. However, organisation and presentation will be achieved by means of tools.

Reference Management Software: EndNote or Zotero will be used to systematically organize and format the citations to all of the references in the format required by the American Institute of Electrical and Electronics (IEEE).

Diagramming and Modelling Software Microsoft Visio or Lucidchart will be used to develop clear pictorial representation of the framework's architecture, its scoring logic flowchart and the maturity assessment process. This helps with rigorous design as well as good communication.

Document Preparation: Standard word processing software (Microsoft Word) will be used for authoring the dissertation in order to professionally format the dissertation.

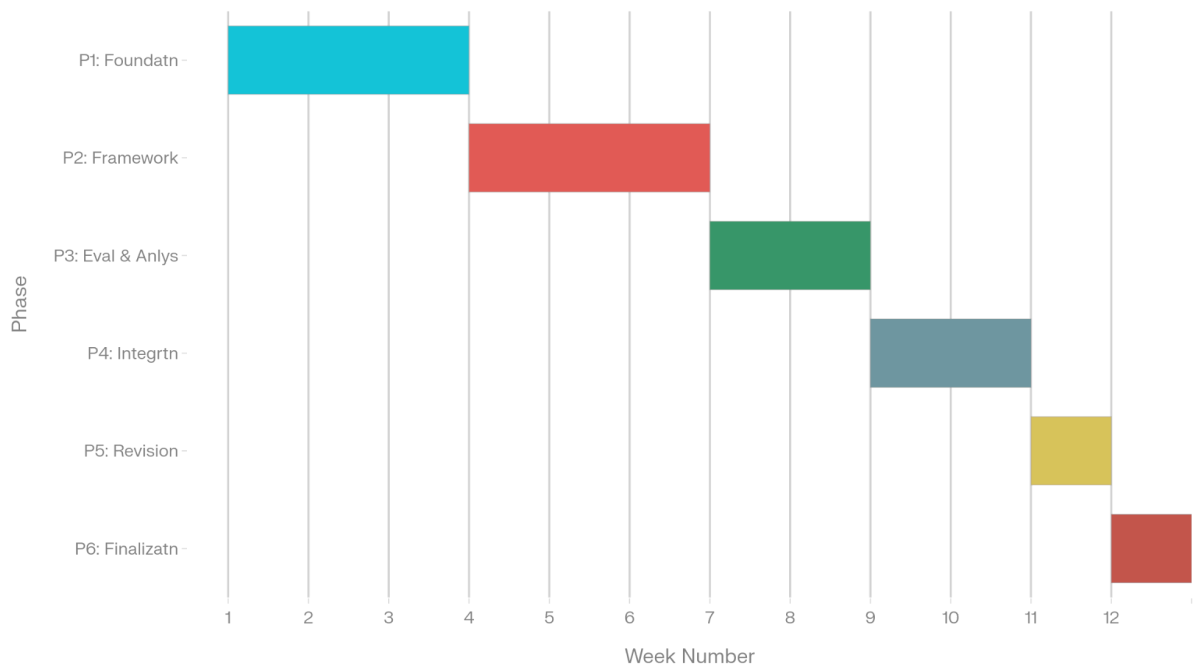
Hardware Requirements: This is a theoretical research so no special hardware (e.g high-performance servers, GPU) are required for this work. Standard computing equipment (laptop/desktop) with internet for retrieval of literature is adequate

Expected Outcomes

This theoretical research is expected to make a few key achievements under the identified deficit of the killer information security governance. The main output will be a complete conceptual maturity framework. This artifact will be a detailed architecture that translates ISO 27001:2022 Annex A controls to a multi-level maturity scale along with clear assessment indicators for each control at each level. A second, very important outcome is the structured, algorithmic scoring mechanism that operationalizes the framework for providing a transparent method of aggregating the control-level assessments into domain and overall Organizational Security Maturity Index (OSMI) scores. Furthermore, the research will result in a collection of theoretical guidelines for the adoption of the framework, its integration into existing ISMS cycles, and its use for continuous monitoring.

The consequences of these results are two-fold. Academically, the contributions of the work are a novel design artifact to the body of knowledge on security metrics and capability assessment, which demonstrates the application of Design Science Research in security governance. Practically, this is a proof of concept tool that organisations can use to tailor to make static compliance data dynamic and thus allow for more strategic, evidence-based decision-making around security investment and prioritising improvement. A major noted weakness of this phase is the conceptual nature of the evaluation; the practical efficacy of the framework and its external validity would need to be empirically tested in the future through case studies or reviews by experts.

Timeline (12-Week Schedule)



Week	Major Phase & Tasks	Key Activities
1-3	Phase 1: Foundation & Problem Finalization	- Conclude in-depth literature review. - Critically synthesise gap in existing models. - Clearly define the research problem and scope;
4-6	Phase 2: Framework Design & Development	- Define architecture of the framework (control set, maturity scale) - Design algorithm for the structured scoring algorithm. Develop Visual Models of the Framework.
7-8	Phase 3: Conceptual Evaluation & Analysis	Put the framework into a hypothetical organizational situation. Develop and analyze sample maturity scores. Critically reflect on the logic and the out-puts of the framework.

9-10	Phase 4: Integration, Writing & Ethics	Putting together and writing the full draft report. Make sure that there is logical flow from section to section. Fill out & turn in the Ethics Form.
11	Phase 5: Revision & Refinement	Proofread, Edit and Revise the draft from self review. Check for formatting, consistency in citation (IEEE) and clarity. Finalize all sections.
12	Phase 6: Finalization & Submission	Perform final checks for academic integrity and submission requirements Submit the final Research Proposal using Turnitin.

This structured 12-week plan ensures a logical progression from foundational research through design, evaluation, and final documentation, keeping the project on track for timely submission.

Conclusion

In conclusion, this research proposal has been able to definition the important gap between static ISO 27001 compliance and dynamic and measurable security maturity by definition a plan to develop and theoretical assess a novel conceptual framework. Through a Design Science Research methodology the project will synthesize available literature, design an integrated maturity model with structured scoring mechanism consistent with Annex A controls and show how to apply integrated maturity model through conceptual evaluation. The result to be expected is a robust artifact that will enable organizations to have a reproducible method of translating compliance data into a strategic maturity index that will address some of the key limitations of inconsistency, poor comparability and a lack of support for continuous improvement. This work aims to both provide a theoretical contribution towards information security governance, and provide a practical basis for facilitating the more evidence-based and strategic management of information security risk.

References

1. Evaluation Information Security Maturity in Higher Education Institutions Using the Kami Index Based on ISO/IEC 27001: A Case Study at University X," *International Journal of Social Science and Human Research*, vol. 8, no. 9, Sep. 2025. [Online]. Available: <https://ijsshr.in/v8i9/86.php>
2. D. Mukti, E. Karnalim, and Y. Heryadi, "Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education," *Indonesian Journal of Electrical Engineering and Technology*, vol. 1, no. 2, pp. 35-44, Apr. 2020.
3. M. A. Rahman, "Cybersecurity Standards in Critical Infrastructure Protection: A Maturity Model for Finnish SMEs," in *Proc. CMS-Conferences*, 2025, pp. 231-245.
4. F. Fitroh, R. Sarno, and K. R. Sungkono, "Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," in *Proc. 2020 Int. Conf. Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, Jakarta, Indonesia, 2020, pp. 174-179.
5. L. K. Sidik and M. Yusuf, "METHODS FOR ASSESSING THE SECURITY OF VIRTUAL NETWORKS AND INFORMATION SECURITY MATURITY MODELS," *Computer Systems and Networks*, vol. 7, no. 2, pp. 45-62, Nov. 2025.
6. A. Alshammari, L. Alazab, and M. Alazab, "Information and cyber security maturity models: a systematic literature review," *Information & Computer Security*, vol. 28, no. 4, pp. 627-644, Jun. 2020.
7. M. H. Ahmadi, "Achieving Excellence in Information Security: A Practitioner's Guide to ISO 27001 Implementation Enhanced with AI and Modern Technologies," *European Modern Studies Journal*, vol. 9, no. 18, pp. 102-130, Sep. 2025.
8. K. Özkan and A. Yavuz, "Exploring the Impact of ISO/IEC 42001:2023 AI Management Standard on Organizational Practices," *Academic Archives of Advanced Research*, vol. 2, no. 15, pp. 45-67, Jun. 2025.
9. R. Thompson and M. Davis, "Pioneering Leadership Dynamics and Security Resilience in Global Project Management: Navigating Complexities in a Volatile Landscape," in *Proc. 13th IPMA Research Conf.*, Vienna, Austria, 2025, pp. 78-95.
10. S. Wijaya, "Preparation of Information Security Risk Management Based on Iso / IEC 27001: 2022 at Diskominfo West Java Province," *International Journal of Management and Humanities Research Review*, vol. 12, no. 1, pp. 234-248, Jan. 2025.

11. A. Youssef and H. Chen, "A Context-Specific Risk Management Model for Data Centers Based on ISO/IEC 27001: 2022: A Case Study of a Government University," in *Proc. 2024 IEEE Int. Conf. Computing and Information Technology (ICCIT)*, Amman, Jordan, 2024, pp. 1-6.
12. P. Anggoro, "Integrating COBIT 2019 and ISO/IEC 27001 for Strengthening IT Governance and Information Security," in *Proc. Conf. Excellence in Social Sciences and Management in the Digital Society (CESSMDS)*, Bali, Indonesia, 2025, pp. 89-104.
13. J. Silva and M. R. Costa, "Information security management: a fuzzy DEMATEL analysis of the new ISO/IEC 27001:2022 controls," *Information & Computer Security*, vol. 33, no. 10, pp. 1245-1268, Oct. 2025.
14. H. Nasution, "Risk-Based Cybersecurity Compliance Assessment System (RC2AS)," *Applied Sciences*, vol. 13, no. 10, p. 6145, May 2023.
15. S. Johnson, K. Lee, and P. Martinez, "A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment," *Mathematics*, vol. 9, no. 9, p. 1045, May 2021.
16. R. Patel and A. Kumar, "A Decision-Making Approach for the Evaluation of Information Security Management under Complex Intuitionistic Fuzzy Set Environment," *Complexity*, vol. 2022, Article ID 9704466, Feb. 2022.
17. M. Sulisty, "Risk Assessment Maturity Level of Academic Information System Using ISO 27001 System Security Engineering-Capability Maturity Model," *Journal of Advanced Engineering Trends and Sciences*, vol. 11, no. 2, pp. 156-168, Jun. 2024.
18. B. Pratama, "Electronic Medical Record Security Assessment Using System Security Engineering–Capability Maturity Model (SSE-CMM)," *Jurnal Informatika Indonesia*, vol. 10, no. 12, pp. 89-103, Dec. 2025.
19. D. Gebremariam, Y. Mekonnen, and T. Assefa, "Maturity of information systems' security in Ethiopian banks: case of selected private banks," *International Journal of Industrial Engineering and Operations Management*, vol. 5, no. 2, pp. 86-103, Jan. 2023.
20. F. Zhao, L. Wang, and X. Chen, "SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs)," arXiv preprint arXiv:2408.16140, Aug. 2024