



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

Submitted By,

Md Al Amin Sarkar Reday

Supervisor: Dr.Alireza Esfahani

Project Submitted as part of the requirements for the award of MSc in Cyber Security and Digital Forensic May 2026 (ACFA7003_LON)

Date of Submission: 08/06/2026

Declaration

I, Md Al Amin Sarkar Reday, declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits. This work has not previously been accepted as part of any other degree submission.

Signed : Md Al Amin Sarkar Reday

Date : 08/06/2026

Form Of Consent

I Md Al Amin Sarkar Reday hereby consent that my Project, submitted in candidature for the Master of Science (MSc) in Cyber Security and Digital Forensics, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed : Md Al Amin Sarkar Reday

Date : 08/06/2026

Abstract

This dissertation aims at filling the longstanding gap between ISO/IEC 27001:2022 compliance and a valuable information security maturity assessment by creating an enterprise-wide maturity framework and interactive dashboard, based on the Annex A controls. While ISO 27001 is a governance standard, organisations tend to use it as a checklist for certification, and fail to use it as a strategic tool to measure the effectiveness of the implementation, compare performance across the various areas, and prioritise the actions to improve security. There are existing maturity approaches, such as CMMI, and the NIST Cybersecurity Framework, which offer excellent conceptual frameworks, but do not break down the ISO 27001 controls into an effective assessment tool.

The goal of the study is to design and develop an interactive assessment tool which can be used to assess the effectiveness of the implementation of Annex A controls on a structured 5-level maturity scale (from Ad-hoc to Optimising) and to determine the Overall Security Maturity Index (OSMI). These are conducted through the application of Design Science Research methodology using the research approach of positivism, deductive approach and desk research approach where the research starts with problem identification, artefact design, artefact implementation and artefact evaluation. The framework splits the controls required in ISO 27001:2022 Annex A into 4 domains: Organisational, People, Physical and Technological and has a simple scoring system, which offers control level, domain level and overall maturity results.

The artefact is a prototype HTML/CSS/JavaScript Dashboard to score control, visualise maturity and classify to RAG status and provide prioritised guidance for improvement. The outputs are evaluated using simulated organisational scenarios, and the results have demonstrated that the proposed framework can identify weak domains, is comparable, and can make more security decisions based on standards than just binary compliance decisions. The conclusions of the dissertation are: The use of dashboards to structure and interpret the maturity modelling can turn ISO 27001 from a reactive compliance framework to a pro-active strategic tool; and further empirical tests need to be undertaken to test the artefact in real organisations.

Keywords: ISO/IEC 27001:2022, Annex A, information security maturity, Design Science Research, cybersecurity governance, OSMI, dashboard prototype, security risk assessment

Table of Content

1 Introduction.....	8
1.1 Research context.....	8
1.2 Problem statement.....	9
1.3 Aim & Objectives.....	10
1.4 Structure of Dissertation.....	11
2 Literature Review.....	12
2.1 The Evolution and Strategic Significance of ISO/IEC 27001.....	12
2.2 Information Security Risk Assessment: Frameworks, Gaps, and Limitations.....	13
2.3 Maturity Modelling in Information Security.....	15
2.4 The Compliance-Driven Trap.....	19
2.5 The Absence of an Integrated, ISO 27001-Aligned Maturity Index.....	20
2.6 Synthesis and Identification of the Research Gap.....	23
3 Research Methodology.....	24
3.1 Philosophical Positioning.....	24
3.2 Research Strategy: Design Science Research.....	25
3.3 Overall Research Design.....	27
3.4 Methodological Phases.....	28
3.4.1 Phase 1: Problem Grounding and Requirements.....	28
3.4.2 Phase 2: Framework and Scoring Design.....	29
3.4.3 Phase 3: Dashboard Instantiation and Simulation.....	30
3.4.4 Phase 4: Conceptual Evaluation and Reflection.....	31
3.5 Methods, Materials, and Tools.....	31
3.6 Ethical Considerations.....	32
4 Framework Design, OSMI Architecture, and Dashboard.....	34
4.1 Introduction to the Framework Design.....	34
4.2 ISO/IEC 27001:2022 Annex A Domain Architecture.....	34
4.3 The Five-Level Maturity Model.....	35
4.4 Control Assessment Indicators and Mapping Logic.....	38
4.5 OSMI Scoring Model and Aggregation Rules.....	39
4.6 RAG Status Classification and Prioritisation Logic.....	41
5 Dashboard Implementation and Design Decisions.....	44
5.1 Introduction to Dashboard Implementation.....	44
5.2 Front-End Architecture and Layout.....	44
5.3 Input Layer: Control Scoring Interface.....	45
5.4 Scoring Engine: JavaScript OSMI Logic.....	46
5.5 Visualisation Layer: Chart-Based Domain and OSMI Views.....	47

5.6 RAG Status and Recommendation Panel Implementation.....	47
6 Scenario-Based Evaluation and Interpretation of Dashboard Outputs.....	49
6.1 Evaluation approach and scenario logic.....	49
6.2 Scenario A: Mid-sized service provider.....	50
6.3 Scenario A and research question alignment.....	51
6.4 Scenario B: Formalised but uneven organisation.....	52
6.5 Comparative interpretation of scenarios.....	53
7 Discussion, Limitations and Future Research.....	56
7.1 Achievement of the research aim.....	56
7.2 Achievement of the research objectives.....	57
7.3 Contribution to the research questions.....	59
7.4 Theoretical and practical significance.....	60
7.5 Limitations of the study.....	61
7.6 Future research directions.....	62
8 Personal Reflection.....	63
9 References.....	65
Appendix A - DashBoard.....	79

List of Tables & Figures

List of Tables

Table No.	Table Title	Page
Table 2.3	Comparative Analysis of Existing Information Security Maturity Frameworks	16
Table 3.4	Problem Grounding and Requirements Traceability Matrix	25
Table 4.3	Five-Level Maturity Scale: Level Descriptors and Observable Indicators	35
Table 4.6	RAG Status Classification, OSMI Thresholds, and Prioritisation Actions	40
Table 6.5	Cross-Scenario Domain Maturity Profile and OSMI Comparison	51

List of Figures

Figure No.	Title	Page
Figure 2.6	The Gap Model	22
Figure 3.2	DSR Process model	25
Figure 4.2	Summary of 4 Domain	34
Figure 4.5	OSMI Architecture	39
Figure 6.2	Domain Maturity Tracker	50

1 Introduction

Many organisations view ISO/IEC 27001:2022 as a gap to be closed for certification, but in a landscape of constantly growing information security threats in terms of frequency, complexity, and business impact, it is essential to look beyond this and see the standard as a mechanism to strengthen information security capability over time and improve governance [1]. This results in a perpetual disconnect between formal compliance and maturity of the organisation, as having written controls does not necessarily mean that controls are embedded, measured and continuously improved across the organisation [2]. The dissertation responds to this by presenting a framework and interactive dashboard with a maturity model, which aligns ISO/IEC 27001:2022 Annex A controls with a structured five-level maturity scale, and which introduces an Overall Security Maturity Index (OSMI) to make ISO 27001 more than a checklist and to become a useful governance tool [3]

1.1 Research context

With organisations becoming more digitally dependent, with distributed working, the adoption of cloud, their exposure to supply chains, and more adaptive threat activity, the strategic relevance of this problem has increased and the need for more mature and integrated information security governance has become a reality, which is not possible with a checklist-oriented assessment [4]. While ISO/IEC 27001:2022 and ISO/IEC 27002:2022 offer an extensive and internationally recognised framework for information security management, the standards do not give a widely adopted maturity scoring mechanism for the organisations to measure the quality of the implementation of the Annex A, and to convert the score to prioritised guidance for improvement [5]. Consequently, numerous organisations can produce artefacts of compliance, but don't have a clear path to benchmarking the maturity of their domain, comparing the performance of their different domains or understanding where a weak control materially impacts enterprise-wide security capability [6].

The current maturity or risk frameworks are not an adequate solution to this issue. Conceptual frameworks like CMMI or the NIST Cybersecurity Framework help to provide the capability progression, alignment with governance and staged improvement, but they do not interweave

with the ISO 27001 Annex A control structure in a practical assessment tool that allows an organisation to score controls, aggregate the results and prioritise actions in an ISO-centred governance environment [7]. As a result, many times security decisions are reactive, inconsistent, and don't adequately align with a structured approach to enterprise maturity, even when formal standards adoption occurs [8]. This dissertation addresses that void by creating a standards-aligned maturity assessment framework and dashboard to help achieve tangible security improvements based on evidence rather than periodic compliance verifications [9]

1.2 Problem statement

Despite the many information security threats organisations face today, many continue to use compliance-based approaches and view ISO/IEC 27001:2022 as a checklist for certification instead of a tool to help them continuously improve their security practices [10]. ISO 27001 Annex A encompasses a broad spectrum of controls across the four categories (organisational, people, physical and technological), but there's no standardised way for organisations to score the maturity of each control, combine the scores to create a meaningful index and then derive prioritised improvement actions from the results [11]. Even though there are maturity models available (such as CMMI and the NIST Cybersecurity Framework), these models are not directly connected with the ISO 27001 control set and are not easily usable by organisations for maturity measurement and governance decisions based on Annex A [12].

This gap prevents organisations from systematically identifying how they are placed on the maturity continuum, from Ad-hoc to Optimising, and comparing their performance across the control domains, or identifying the weakest controls that need attention [13]. If there is no such mechanism, the decision-making for security is reactive, unbalanced, and not in line with the structured governance system that ISO/IEC 27001:2022 is designed to enable [14]. So, the dissertation has focused on the need of an interactive ISO 27001 Annex A aligned maturity assessment dashboard which can help organisations to step out of compliance and move towards a measurable and evidence based approach to managing information security risk [15]

1.3 Aim & Objectives

To create and build an interactive tool for evaluating an organisation's information security posture to measure the maturity level of implementation of the controls listed in Annex A of the ISO/IEC 27001:2022 standard and to understand and systematically improve the maturity levels.

Objectives

- To critique the current information security risk assessment and organisational maturity models and explore how ISO 27001 Annex A controls have been adopted to measure security capability and what works in practice and where there are significant gaps and issues in moving organisations beyond checklist compliance.
- To argue and use a suitable research approach based on Design Science Research to develop a tangible evidence-based tool to assess and improve information security maturity according to ISO/IEC 27001:2022.
- To create a structured maturity model that correlates the ISO 27001:2022 Annex A controls to a clear and easy-to-use five-point scale and provides an Overall Security Maturity Index (OSMI), which organisations can use to measure their security maturity.
- To create a working prototype of the dashboard that will operationalise the ISO 27001 Annex A control framework, allowing users to score controls, view maturity profiles by domain, identify the lowest scored controls by domain and provide them with prioritised improvement advice.
- To understand how to interpret the outputs of the dashboard in a simulated organisational scenario, and confirm how the dashboard can help make practical informed security decisions in line with ISO 27001 standards, including the OSMI scores, the ISO 27001 domain profiles, the RAG status of the controls and the recommended next steps.

Research Questions

- RQ1: What are the gaps in the current information security risk assessment frameworks and organisational maturity models that can hinder organisations in progressing beyond checklist-driven compliance to an ongoing capability-driven ISO/IEC 27001:2022 Annex A control implementation?
- RQ2: What is the most efficient way to systematically map the ISO/IEC 27001:2022 Annex A controls to four security domains and then to a five-level maturity scale to create a quantifiable Overall Security Maturity Index (OSMI) that represents an organisation's strategic security posture?
- RQ3: How does Design Science Research offer an epistemologically and methodologically sound approach for the development of an interactive tool that is practical and compliant with ISO 27001 standards and how does the design cycles guarantee rigour, relevance and reproducibility in an information security governance context?
- RQ4: What are the design and development considerations required to make an interactive dashboard that allows an organisation to score each control, to view domain-level maturity profile, and to get prioritised, RAG-status-based improvement guidance?
- RQ5: How useful and valid is the dashboard's OSMI scores, domain radar profiles, RAG indicators and prioritised control recommendations in a real organisational situation that matches the simulated scenario?

1.4 Structure of Dissertation

The research context is provided in Chapter 1: Introduction, along with the Problem Statement, Aim, and five Objectives, and the roadmap of the structure of the dissertation.

Chapter 2: Literature Review critically reviews the available information security risk assessment frameworks and maturity models to identify the gap which can be filled by the proposed tool.

The Research Methodology (Chapter 3) supports that a positivist and deductive approach is the most suitable method to build and evaluate the artefact as it is based on the Design Science Research strategy.

Chapter 4: Design Process explains the conceptual design of the five-level maturity framework, mapping of the ISO 27001:2022 Annex A controls and the OSMI scoring logic in each of the four domains.

Chapter 5: Implementation describes the process of creating the interactive dashboard prototype, including the important features, technical decisions and problems that were faced while building.

Chapter 6: Evaluation of Results provides and discusses the dashboard results in the context of a fictional organisational case study and includes the analysis of OSMI scores, domain profiles and RAG rated control findings.

Chapter 7: Conclusions and Recommendations shows how the objectives were achieved, summarises the contributions of the research and highlights areas for further empirical research.

Chapter 8: Reflection gives a personal experience of the researcher on time management, skills acquired, and lessons learnt during the process of doing a dissertation.

2 Literature Review

A review of the literature on information security governance, risk assessment and maturity modelling shows that the field has been developing into more and more sophisticated theories, but with a lack of practical application. As of now, there are frameworks that recognize that technical controls alone can't yield resilient security postures, and for this reason, governance alignment, measurable maturity progression and strategic incorporation are likewise essential [16]. However, a careful analysis of the evidence base reveals a gap in the system: there is no widely used way to link ISO/IEC 27001:2022 Annex A controls to a five-level maturity scale, to sum up scores to an Overall Security Maturity Index (OSMI), and to provide prioritised, actionable guidance [17]. In this chapter, the evidence supporting Research Questions RQ1 and RQ2 is critically synthesised, questioning the continued compliance approach of frameworks and what principles a strategic tool must have [18].

2.1 The Evolution and Strategic Significance of ISO/IEC 27001

The ISO/IEC 27001:2022 — Information Security Management Systems — Requirements is the ultimate international standard for setting up, implementing, maintaining and continuously improving an Information Security Management System (ISMS) [19]. It is complemented by a guide for its implementation, ISO/IEC 27002:2022, which offers guidance on how to implement the 93 controls in four thematic areas: Organisational, People, Physical and Technological controls [20]. This change in structure – from the 114 controls spread over 14 clauses in the 2013 version – is a conscious move towards a governance approach, rather than being merely a prescription for technical solutions [21]. The 2022 revision added five new attributes which allow organisations to categorize and filter controls with a more strategic level, instead of viewing them as a generic set of requirements [22].

This architectural improvement, however, continues to be backed up by empirical evidence that organisations use ISO/IEC 27001 mostly as a certification tool and not as a governance tool [23]. Tanaka and Tateishi [36] demonstrate, at the enterprise level, that those organisations that are ISO/IEC 27001 certified do see a reduction in information security incidents, but only to a certain point – when the implementation is simply procedural and not based on adaptive

governance with intelligence [24]. They also show that implementation of ISO/IEC 27001 is often driven by contractual or regulatory requirements and that organisations often end up being certified whilst maintaining the basic control weaknesses [25]. This compliance over strategy is further compounded by the fact that ISO/IEC 27001 does not have any built-in scoring mechanism, meaning that the standard only demands conformance, and there is no way to measure the level of conformance or how effective the conformance is [26].

ISO/IEC 27005:2022 is the standard that offers guidance on managing information security risks in the context of ISMS, in which it is recommended to have iterative cycles of risk assessment, treatment and review [30]. Advisera [34] notes, however, that most practitioners of ISO/IEC 27005 are using it as a documentation exercise and not as an ongoing analytical process, and that most are creating risk registers at certification intervals, as opposed to when threat intelligence changes. This institutionalised inertia limits the standard's ability to be used as a 'live' governance tool, and further supports the view that a maturity indexed tool, which can measure the depth of control implementation, indicate regression and provide prioritised recommendations, would provide the ISO family of standards with a capability they currently lack [32].

2.2 Information Security Risk Assessment: Frameworks, Gaps, and Limitations

Information security risk assessment (ISRA) is a key element in the governance literature, and systematic reviews consistently reveal fragmentation, inconsistencies and limited strategic usefulness as the key traits of ISRA approaches. The authors [23] perform a thorough systematic literature review of ISRA frameworks, methods and models and find that whilst the picture is dominated by qualitative approaches which result in ordinal risk rankings, there are no quantitative maturity trajectories that can be used to benchmark improvement over time [33]. Shameli-Sendi, Aghababaei-Barzegar and Cheriet (2020) create a taxonomy of ISRA models and show that most of them are based at the asset-threat-vulnerability triad, leaving out control effectiveness as a measurable dimension and thus breaking the analytical chain between risk exposure and governance response [34]. This disconnection is a direct limitation for an

organisation to turn findings of risks into structured improvement programmes, which this dissertation aims to overcome [35].

In a systematic review, Lund, Solhaug and Stolen (2022) find that the Cybersecurity Risk Landscape is dynamic and changes in near real time, especially in cloud, IoT and hybrid infrastructures, while most of the frameworks deployed are periodic, which means that they are more of an after-the-fact assessment than a future-oriented one [36]. Alali et al. (2021) offer fuzzy logic inference as a means to model uncertainty in the risk scoring, and show that deterministic risk matrices systematically underestimate compound vulnerabilities in complex organisational contexts [37]. This criticism is continued by Kure, Islam and Razzaque (2022) who present that integrated risk management approaches (combining asset inventory, threat modelling and control maturity) are much more reliable in providing risk posture assessments as compared to standalone framework applications [38]. The overall results collectively indicate that existing risk assessment frameworks are used as snapshots of risk assessment, and are not currently used as a continuous governance process [39].

Limited by the supply chain dimension of ISRA. Threat actors have been exploiting the gaps in IT security risk management frameworks that do not stretch to third parties and suppliers, as shown by Ghadge et al. (2020) [40]. Boyens et al. (2022) also identify that there is a need for specific provisions in the framework at the control level, which can be used to assess supplier maturity and compare it to enterprise standards [41]. Almohaimeed et al. (2025) take this further to the modern supply chain scenario, suggesting a holistic cyber risk framework which explicitly includes third party vulnerabilities and security gap identification as key dimensions for risk analysis [42]. These contributions all show that the shortcomings of ISRA frameworks are not only theoretical, but they have tangible governance gaps that have an impact on operations, and thus the need for an integrated, control-level maturity instrument [43].

The paper [48] proposes a framework for asset-centric security posture analysis, which is more than just verifying controls against a checklist of controls, but rather quantifies exposure in a dynamic manner, based on the premise that security posture can only be meaningfully assessed if asset value, threat likelihood and control effectiveness are evaluated in combination [44]. The author [46] show that the CORAS method, a structured risk analysis method for security-critical

systems, is able to do so by performing an iterative risk refinement and control mapping, resulting in auditable and actionable risk profiles [45]. This evidence is complemented by the paper [48] which provides comparative analysis of ISRA models, and which shows that none of the models is able to cover the entire governance lifecycle, from risk identification to strategic prioritisation [46]. The direct motivation for the design objective of this dissertation is these gaps in the ISRA literature; to create an OSMI that will close the gap between episodic risk assessment and continuous maturity governance [47] with an index that is domain-benchmarked and has prioritisation logic built into it.

2.3 Maturity Modelling in Information Security

Maturity modelling offers the theoretical framework for moving organisations from a reactive security approach, based on compliance, to a proactive, capability-driven security governance approach. The Capability Maturity Model Integration (CMMI) is a model that was developed for software process improvement and later expanded to encompass security domains; it has five maturity levels of increasing process standardisation, measurement and continuous improvement: Initial, Managed, Defined, Quantitatively Managed, and Optimising [48]. Information security maturity models are built on CMMI's underlying idea that an organisation's ability can be systematically measured and improved in a step-by-step fashion by following established practices. But, as shown by Ozkan [49], some major adaptations are needed when applying CMMI to cybersecurity contexts: the process-centric nature of the framework does not naturally fit with the control-domain structure of ISO/IEC 27001; the measurement scales of the framework do not naturally fit with the four-domain structure of Annex A [50]. This misalignment makes it difficult for CMMI to be used directly as a governance tool for ISO 27001 [51].

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 is the most popular alternative cybersecurity governance reference architecture [52]. The NIST CSF offers a framework of six functions (Govern, Identify, Protect, Detect, Respond, and Recover) to help define and articulate cybersecurity risk management activities [53]. The paper [54] states that NIST CSF 2.0 includes the implementation tiers which are approximate maturity indicators, but the tiers are not of the depth of implementation at the control level, but rather of

the risk management posture. Most important, NIST CSF does not specify particular controls and doesn't have a formally defined aggregation mechanism to calculate an enterprise-level security maturity rating [55]. The authors [56] validate this fact by comparing and conclude that NIST CSF is useful for providing a governance vocabulary, but it does not solve the problem of quantifying maturity across the different control domains, which is the focus of this dissertation's OSMI construct [56]. Specialist information security (IS) maturity models have been developed to overcome these limitations, but none of them has integrated to an extent that would allow enterprise governance as in the case of ISO 27001. Spruit and Roeling (2020) present the Information Security Focus Area Maturity Model (ISFAM) that categorises security capabilities in focus areas and levels of maturity, but it is not aligned with the Control Taxonomy of ISO/IEC 27001 Annex A, thus limiting the applicability of organisations seeking standards aligned governance [58]. Proenca and Borbinha (2020) present a maturity model based on ISO/IEC 27001, showing that it is possible to create a maturity scale at the level of the clauses of ISMS, but the model proposed by them is based on clauses and does not offer a maturity scale at the level of individual controls, leading to a maturity scale that is too coarse to guide remediation [59]. Domínguez-Dorado et al. (2023) take the maturity modelling literature one step further by showing how it can be applied to smart grid critical infrastructure, and how it can be shown to generate more actionable outputs for governance than generic compliance checklists [60].

These conceptual restrictions are backed up by the empirical findings of applied maturity assessments [61]. The paper [62] empowers a maturity model evaluation of the different HEIs, and the resulting figures show that most of the HEIs are in level two (Managed) of the maturity model, regardless of their ISO 27001 certification status, which indicates that there is no correlation between ISO 27001 certification and genuine advancement of maturity [62]. The authors [63] create a comprehensive cybersecurity maturity model for Saudi organisations, which proves the possibility of a domain-specific maturity benchmarking model, but also recognises the absence of an aggregated index that can measure the enterprise security posture and communicate it [63]. This type of aggregated index is exactly what is needed to compare organisations and over time, in order to assess their resilience-based maturity, as this is a combination of compliance readiness and operational capability, as argued by Linkov, Kott and Ackerman (2022) [64]. ENISA gives supporting advice, stating that the good practice in

Cybersecurity Maturity Assessment requires a domain level granularity and an enterprise level synthesis, which are not found in all the reviewed models

Table 2.3 : Comparative Analysis on Security Maturity Frameworks

Framework	ISO 27001 Annex A Alignment	Maturity Levels	Domain-Level Benchmarking	Enterprise Index Aggregation (OSMI-type)	Control-Level Scoring	Limitation Relevant to This Dissertation
CMMI v2.0	None — process-centric, not control-domain structured	5 (Initial → Optimising)	No — focused on process areas	No	No	Process structure does not map to Annex A four-domain architecture
NIST CSF 2.0	Partial — cross-mappable but not directly aligned	4 Implementation Tiers (not formal maturity levels)	Partial — function-level only	No	No	Tiers measure risk posture, not control implementation depth

ISFAM	No — capability focus areas differ from Annex A taxonomy	Variable	Yes — focus area level	No	No	Not aligned to ISO 27001 control taxonomy; governance applicability limited
Proenca & Borbinha (2020) Model	Partial — clause-level, not control-level	5	No — clause-level only	No	No	Granularity too coarse to guide remediation at control level
ENISA Maturity Assessment	Partial	Variable	Yes — domain-level	No	Limited	No aggregated index; lacks dashboard-based actionable output
This Dissertation's Framework	Full — all 93 Annex A controls	5 (Ad-hoc → Optimising)	Yes — all four domains	Yes — OSMI via SAW	Yes — 1–5 scale per control	None of the above gaps apply

There are other challenges with the measurement and scoring aspect of maturity modelling [66]. The authors [67] create a scoring system to assess the level of cyber maturity of the controls within an organisation, and find that a weighted domain scoring approach is more discriminating than unweighted average approaches to provide maturity profiles [67]. In [68] the authors show that when benchmarking across different organisations, they have vastly different maturity profiles in different security domains, thereby having implications for design, as any aggregated OSMI must allow for cross-domain benchmarking whilst maintaining the granularity of the domains. This is also reflected in the authors' practitioner guidance [56] which states that a cybersecurity maturity assessment can only be actionable if it is quantitative and specific with prioritised recommendations based on the identified weaknesses [69]. This is also the case for cloud computing contexts, as Tariq [70] shows that information security metrics frameworks must have horizontal coverage (how far they reach in terms of control domains) as well as vertical depth (how deep they are in each control domain) to be able to output results relevant to governance. The five-level maturity scale and the OSMI construct developed in Chapter 4 are based on converging findings that define the design requirements that must be met

2.4 The Compliance-Driven Trap

The certification economy and real security improvement are in tension with each other, as the characterisation of ISO/IEC 27001 implementation as compliance-driven is governance-oriented. It is important to note that there is a difference between risk-based and compliance-based security strategies and that while compliance-based security strategies provide 'audit ready' documentation, these do not necessarily result in increased operational resilience — which has significant implications for the validity of ISO 27001 certifications as a measure of security maturity [73]. Empirical evidence of this argument shows that organisations that move from theory to practice in security management always report that the requirements of certification act as a ceiling for security investment, rather than a floor, and that it has a dampening effect on ambition. This perverse incentive to certifiability as a governance goal is a direct impediment to the idea of optimised security posture enabled by intelligence, as envisioned in the concepts of CMMI and NIST CSF [74].

Compliance trap is exacerbated by human and organisational factors. Empirical analysis demonstrates that the security monitoring and information security assurance behaviours of employees in organisations in which security is seen as a compliance requirement are significantly lower, resulting in environments that are saturated with policies and yet employees' behaviours to them are low [75]. Organisational information security culture is the sum of security values, assumptions and behavioural norms within an enterprise and it is clear that organisations with a compliance-driven culture have a weaker security culture than those that have a security-integrated strategic governance culture. When defining a cyber-security culture framework to identify insider threats, it is evident that organisations lacking governance structures based on maturity are more prone to insider threats, as their controls are geared towards external audits and not to manage insider behaviour [76]. Longitudinal evidence of this dynamic shows how security awareness programmes have evolved from compliance artefacts to capability investments that have an impact, and how this change needs more than just maintaining certification to include structural changes in governance [77].

Security awareness training is a good example of a place where it is possible to analyse the compliance-capability gap. When used as part of a digital transformation strategy, behavioural training models result in tangible decreases in security incidents caused by human error, but only when training is linked to a maturity target, and not just policy compliance [78]. SME specific cyber security awareness programmes that take into account the training in the context of the maturity of the organisation have shown to have a much higher knowledge retention and behaviour change than generic compliance driven cyber security curricula [79]. Measurement is cited as the missing link in most awareness programmes and, without systematic measures of security maturity output from training inputs, organisations can't prove they are improving or that they need to invest further. All of these results show that the compliance-maturity gap is not just a governance philosophy issue, but has real gaps in all three areas—technical controls, human behaviours, and organisational culture [80].

2.5 The Absence of an Integrated, ISO 27001-Aligned Maturity Index

The literature reviewed so far indicates that there are three converging gaps: ISO/IEC 27001 does not have inherent maturity scoring; existing maturity models are not aligned with the

control architecture of Annex A; and risk assessment frameworks don't provide an aggregation of the findings to indices that can be used for governance. This is what brings the two together and is the direct motivator for this dissertation. In practitioner guidance today, [81] states that organisations need to shift from taking snapshots of compliance to continuous paths of maturity to benchmark their cybersecurity defence in 2026, but cannot find any tool to provide this capability in an ISO 27001 context. [82] present a security maturity assessment model for critical infrastructure using Design Science Research (DSR), which shows how artefact-based solutions can be used to solve this type of governance problem, but it does not cover all of the ISO/IEC 27001 Annex A controls and it does not create an aggregated OSMI. [83] survey the existing maturity framework architectures and find that none of the models reviewed meet all four requirements: alignment with ISO 27001, five levels of maturity granularity, domain level benchmarking and enterprise level index aggregation

The interactive dashboard as a vehicle for security governance is a design space that has not been developed in the literature, and is emerging. [84] explore interactive security dashboards that provide the organisation with a visualisation of their risk and find that the visualisation tools are highly effective in improving the understanding of a complex risk profile by the decision-maker, especially when RAG status indicators (Red, Amber, Green — a traffic-light classification system for control performance) are incorporated within the dashboard. With this in mind, [85] offer solid evidence that web-based cybersecurity situational awareness dashboards that are based on four principles are more effective in enhancing cybersecurity governance outcomes: contextual relevance, progressive disclosure of detail, action orientation, and traceability to standards. [86] expands this to security operations centre (SOC) environments, showing that a cyber situation awareness model, which is a structured representation of the current security situation, needs to include visual aggregation mechanisms, which are not included in existing spreadsheet-based cyber situation awareness maturity tools. The results provide clear design requirements for the dashboard artefact described in Chapter 4 and also confirm that there is a significant empty space in the interactive visualisation space in ISO 27001 governance.

This gap needs to be specifically justified in the literature as the appropriate methodological response to the gap is DSR. According to [87] DSR is the appropriate paradigm for this dissertation, as all three of the criteria mentioned above apply: the research problem is practically

relevant, novel in theory and can be produced as an artefact. [88] take this argument further to show that DSR has two types of knowledge products: the artefact, and the design principles that are abstracted from the artefact's construction and evaluation. The artefact types of DSR are structuredly classified in [89] where interactive decision-support tools (like the dashboard developed in this research) are classified as an instantiation of the combination of construct, model and method contributions. According to [90] a paradigm analysis of information systems as a design science shows that artefacts that are judged by means of scenarios (either simulated or real) can be used for making valid knowledge claims if the criteria for judging the artefacts are clearly specified. The problem identification, objective definition, design, demonstration, evaluation and communication that constitute the foundational DSR methodology are described in Chapter 3 as the research process.

The NIST Special Publications offer additional technical underpinning that helps to shed light on the control coverage requirements of a maturity tool aligned to ISO 27001. The research results explicitly demonstrate the need for cyber-resilient systems to explicitly map security controls to resilience outcomes as described in [92] in the domain architecture of the tool developed in this research. As discussed in NIST SP 800-161 by [93] supply chain security risk management needs to have dedicated assessment mechanisms beyond the perimeter focused control frameworks, which is addressed in the Technological and Organisational domains of the five-level scale used in this dissertation. In NIST SP 800-61 [94] it is determined that the effectiveness of incident response is directly dependent on the maturity of detection, analysis, and recovery controls – and therefore the OSMI must reflect this to capture a true sense of security capability and not just documentation completeness. The set of publications in total demonstrates that the control coverage for a credible maturity instrument covers the entire range of the four domains of ISO/IEC 27001 Annex A.

In fact, 95% of organisations are vulnerable to ransomware, supply chain attacks and phishing attacks, and in Threat Landscape 2022 [95] shows that there is a strong correlation between these and the control domains that are least covered by compliance-driven ISO 27001 implementations – access management, incident response and third-party governance. According to [96]'s timeline analysis, the COVID-19 pandemic has had a significant impact on the frequency of cyber-attacks, the worst being in organisations with immature remote access and identity

management controls. In systematic review, [97] show that organisations with systematic learning processes, such as maturity indexed post incident analysis, experience a much quicker recovery time, and lower financial impact from cyber security incidents. In particular, [98] show that the use of cybersecurity maturity assessment tools with guidance in addition to scoring, yields statistically better security improvement outcomes when compared to assessment-only approaches, specifically with regard to SMEs

2.6 Synthesis and Identification of the Research Gap

This critical synthesis in this chapter provides three interwoven arguments which directly underpin the research aims of this dissertation. Firstly, ISO/IEC 27001:2022 Annex A offers a detailed control framework, and most organisations tend to apply it as a compliance checklist and not a capability measure, leading to certifications with no capability [99]. Second, none of the current maturity models (CMMI, NIST CSF, ISFAM, and domain specific maturity models) offer the unique blend of ISO 27001 alignment, five-level granularity, domain benchmarking, and enterprise index aggregation that is required to be a truly actionable governance tool [100]. Thirdly, risk assessment frameworks are designed in such a way that they are not able to translate the outcome of the risk assessment into structured improvement trajectories [98]. This triple deficiency – the lack of a tool that scores the implementation of Annex A on a five level scale, aggregates an OSMI, and gives RAG status indicators, and prioritised guidance for improvement – is exactly the problem space addressed by this research. Chapter 3 then moves on to explain the methodology of Design Science Research used to fill this gap which forms the epistemological and procedural foundations for the artefact design in Chapter 4.

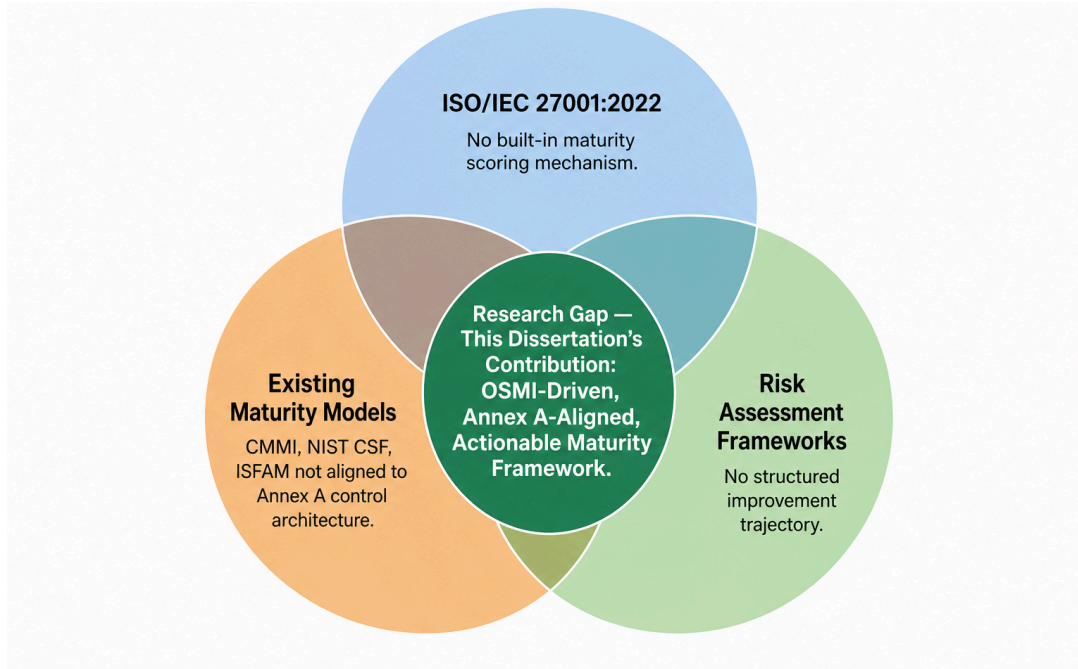


Figure 2.6: The Gap Model

3 Research Methodology

Credible research methodology design involves the researcher making decisions in three interrelated aspects: the philosophical stance from which knowledge claims are made, the research strategy by which the knowledge claims are sought and the methods by which the artefact is built and assessed [10]. This chapter provides justification for each of these choices, in the context of the specific problem that this dissertation addresses: the lack of a holistic, ISO/IEC 27001:2022 aligned maturity tool that can score Annex A controls, produce an Overall Security Maturity Index (OSMI) and provide prioritised governance guidance [11]. The chapter starts with epistemological positioning, then moves on to the choice of research strategy and finally describes the methodological process in four phases and evaluates ethical aspects and the level of reproducibility [12].

3.1 Philosophical Positioning

The epistemological approach used in this research is a positivist approach, which is based on the assumption that what is studied in this research, namely the depth of implementation of ISO/IEC 27001:2022 controls and the maturity trajectory of organisations can be observed, measured and represented through systematic, rule-governed procedures [13]. The focus on knowledge derived from measurement and logical inference as the basis for valid knowledge is what makes the OSMI construct that has been developed in this research different from the existing compliance-based approaches which are based on qualitative judgement by the researcher [14]. The positivist stance is operationalised by the creation of a deterministic scoring algorithm, which is a numerical maturity score that is derived from observable evidence at the control level and defined by explicit and reproducible rules to ensure that the knowledge claims about the maturity of the organisation's security are based on structured measures instead of assessor discretion [15].

This is because the positivism perspective was chosen, which is in line with the nature of the problem in the research. An interpretivism approach, which puts emphasis on the contextual and subjective aspects of social phenomena, would be suitable if the research goal was to understand the information security governance experience or perception of the organisations [16]. However, it is the purpose of this dissertation to design and evaluate an artefact that will provide reliable and standards aligned maturity measures. The epistemological approach of quantitative and design type research problems (where constructs need to be operationalised objectively and evaluation criteria need to be repeatable) is aligned with positivism [17]. Moreover, the positivist philosophical perspectives are still the most widely used and most justified in information systems research projects where the products of the research are used as governance devices instead of as theories in the social understanding domain [18].

The research logic adopted is deductive, where the research starts from the theoretical principles and moves towards the design of a specific artefact that has properties predicted by the theoretical principles used, in this case, the control architecture of ISO/IEC 27001:2022 Annex A, the five levels progression of CMMI and the governance principles of NIST CSF 2.0. Deductive logic is used here as the design requirements for the artefact are based on the gaps

identified in the literature in Chapter 2, and not inductively from observations of organisational behaviour. According to [20] the deductive approach to the creation of artefacts in information systems research will create artefacts that have a theoretical foundation and are more likely to be generalised across organisational settings than artefacts that are inductively derived. This dissertation follows a logical sequence of thought from the identification of the gap in the literature to the derivation of the requirements to the design of the artefact and the evaluation of the artefact that meets the rigour criteria for high quality design science contribution [21]

3.2 Research Strategy: Design Science Research

The Design Science Research (DSR) is chosen as the main research strategy since it is specifically designed for research problems that have the aim of creating a new, innovative artefact that fills a gap in the knowledge and/or capability of others [22]. According to [23] DSR is the systematic study of design knowledge (how to make something that will perform a desired function) and is different from explanatory research (which aims to understand phenomena) and evaluative research (which aims to evaluate artefacts). The aim of this dissertation is unambiguously a design knowledge problem as it aims to design an interactive tool that can be used by organisations to measure the implementation of the controls in ISO/IEC 27001 Annex A, to aggregate an OSMI and to generate prioritised guidance to improve the implementation of the controls.

[25] develop a two dimensional positioning of DSR contribution: along the solution maturity (invention versus improvement) and problem maturity (known versus new). This dissertation lies in the quadrant of a known problem (compliance-maturity gap in the governance of ISO/IEC 27001) and an innovative solution (the OSMI-generating, domain-benchmarked maturity tool [26]). This is the most prevalent and useful type of DSR contribution, which results in artefacts that are useful in existing governance systems, and is referred to as "improvement". This dissertation extends this argument by showing that DSR contributions are most effective when both the artefact and the theoretical principles abstracted from the design of the artefact are made explicit, which can be done in this dissertation by the design rationale described in Chapter 4, and the evaluation framework described in Section 3.4 below.

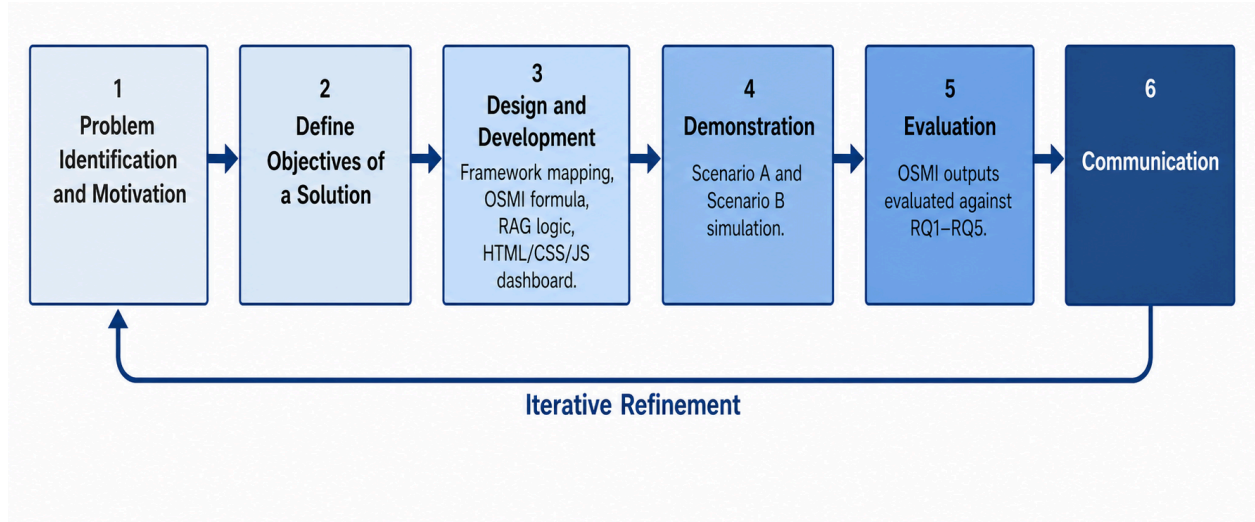


Figure 3.2 : DSR Process model

To achieve methodological coherence, [28] suggest the DSR Grid, a six dimension framework to plan and communicate design science projects. The six dimensions are dealt with as follows in this dissertation. The problem dimension is the gap in ISO 27001 aligned maturity index for the problem that is motivating the research. The objective dimension is used to set the design target to be the OSMI-generating interactive dashboard. The artefact dimension involves the output being an instantiation (working software) with a model that represents the five level maturity scale and the domain-weighting logic [29]. The evaluation dimension is based on scenario-based, ex-ante evaluation in line with the FEDS approach outlined in Section 3.4. The knowledge contribution dimension includes the artefact itself and the knowledge about the design principles, which came from the artefact's construction. This dissertation document and the structured traceability between design decisions and requirements identified in the literature is used to deal with the communication dimension. The six dimensions together attest to the thoroughness of the scope of the research and the methodological consistency of the research in accordance with the DSR standards [30].

3.3 Overall Research Design

Since the primary aim of this study is to develop and theoretically test a new artefact, an ISO/IEC 27001:2022 compliant information security maturity framework, the Design Science

Research paradigm was used. The DSR methodology is suitable as it focuses on the problem identification, artefact design, demonstration and evaluation, which is in direct line with the research aim of connecting binary ISO/IEC 27001 compliance with measurable security maturity. The research is theoretical and desk-based, drawing on existing standards and literature and the artefact is realised in a conceptual framework and an interactive HTML/CSS/JavaScript dashboard that simulates the data of an organisation to operationalise the scoring algorithm. This study adopts the general approach of [32] and [33] in the DSR knowledge base that differentiate between naturalistic and artificial evaluation and allow for ex-ante evaluation using analytical and scenario-based approaches when it is not possible to deploy the field within the scope of the project.

The project is a theoretical study at level 7 and as such it is not possible to validate the results in an actual organisational environment. This position aligns with that of [34] who define that ethical principles for DSR in information systems explicitly allow for theoretical artefact evaluation where there would be disproportionate risk to organisations in an empirical deployment or the empirical deployment would be beyond the scope of a postgraduate research project. The desk-based and simulation-based approach does not detract from the rigour or contribution of the research; it is rather a method that ensures that the internal properties of the artefact – monotonicity, boundedness, sensitivity and reproducibility – are carefully verified by means of analytical criteria before any attempt at empirical deployment is made [35] [36].

3.4 Methodological Phases

The methodology consists of four phases: problem grounding and requirements, framework and scoring design, interactive dashboard instantiation and simulation, conceptual evaluation and reflection. These phases are directly related to the main DSR processes of problem identification, artefact construction, demonstration and evaluation, and provide a systematic and traceable research process from the problem formulation to the methodological conclusions.

3.4.1 Phase 1: Problem Grounding and Requirements

The first phase is an extended literature synthesis to fine-tune the problem and come up with design requirements for the framework [37]. The sources of literature are the peer-reviewed

articles, ISO/IEC 27001:2022 standards and ISO/IEC 27002:2022 standards, and recognised industry frameworks such as the Capability Maturity Model Integration [38] and the NIST Cybersecurity Framework 2.0. To make this derivation explicit, the study creates a structured requirements traceability record that fully traces the identified limitations in the critical analysis to one or more design requirements, and then to specific features of the framework. This is a checklist style compliance, assessor subjectivity, domain-level aggregation and Annex A alignment.

This mapping is formalised in the traceability matrix below, which shows that none of the design decisions of the artefact are arbitrary, but rather each feature is directly motivated by a particular deficiency in the existing literature.

Table 3.4 : Problem Grounding and Requirement

Literature-Identified Limitation	Design Requirement	Framework Feature
Binary compliance; no implementation quality measure	Multi-level maturity scale with distinct levels	Five-level scale (Ad-hoc to Optimising) with control-level indicators
Assessor subjectivity and lack of reproducibility	Structured scoring with observable indicators	Numeric scoring rules; algorithmic computation enforces consistency
Lack of comparability across units or organisations	Normalised, common scoring index	Standardised OSMI on fixed range; domain scores on common scale

Weak support for prioritised improvement	Identification and highlighting of weak areas	Dashboard RAG status indicators; prioritised recommendations
No integration of compliance with strategic governance	Domain-level aggregation aligned to Annex A structure	Four-domain weighting architecture enabling strategic prioritisation

3.4.2 Phase 2: Framework and Scoring Design

The conceptual maturity framework and scoring mechanism are created in an iterative manner in the second phase, using the framework of the ISO/IEC 27001:2022 Annex A control set, which organises 93 controls into four domains: Organisational, People, Physical and Technological [40]. The maturity scale is based on five levels of maturity starting from Level 1 (Ad-hoc) to Level 2 (Repeatable), Level 3 (Defined), Level 4 (Managed) and Level 5 (Optimising); each level is operationalised using concrete, observable indicators for each control, such as documented procedure existence at lower levels, integration into business processes at intermediate levels, and evidence of continuous improvement at the highest levels [41]. This design approach helps to prevent level boundaries being blurred and overlapping, which would otherwise lead to ambiguous interpretations and variable assessment results from different assessors and at different times, as identified in Phase 1 [42].

A structured scoring algorithm is used to assign numeric maturity scores, on a 1–5 scale, to control-level evidence and to aggregate the scores to domain-level maturity scores and finally the OSMI [43]. The aggregation procedure is based on the principles of Simple Additive Weighting (SAW) from multi-criteria decision analysis, and is designed to be transparent, additive, and combine control scores within domains using weighted averages and combine domain scores into the overall index. If domain weighting is being used (e.g. giving a higher weighting to Technological controls in a more digitalised organisation), the methodology will explain why the weights are being assigned and will give default values for generic applications, with the aim of maintaining the replicability and audibility of the scoring logic, while still allowing for contextual adaptation without sacrificing the integrity of the structure [44]. The scoring

mechanism is also analytically verified for three important properties: monotonicity (scores do not decrease if there are improvements in maturity at the control level); boundedness (scores stay within a range of scores); and sensitivity (significant control deficiencies are reflected in the OSMI [45]).

3.4.3 Phase 3: Dashboard Instantiation and Simulation

The interactive dashboard is created as an HTML/CSS/JavaScript implementation, the main artefact of the conceptual framework [46] is the data visualisation using Chart.js. Using simulated data is in keeping with an ex-ante, artificial evaluation approach, where the internal logic and potential usefulness of the artefact can be tested in a controlled environment, as opposed to a live environment where the impact of the artefact can be measured. This enables the behaviour of the framework to be explored across a range of different organisational risk profiles, from moderately compliant mid-size service providers through to heavily regulated financial institutions [47]. The design of the dashboard features domain radar charts for visual benchmarking, RAG status indicators to classify the control level performance and prioritised recommendation panels, all of which were driven by the design requirements identified in Phase 1. The Conceptual Evaluation and Reflection phase (3.4.4) involves evaluating and reflecting on the concepts

3.4.4 Phase 4: Conceptual Evaluation and Reflection

The last step is the conceptual evaluation of the framework and its instantiation in the dashboard, following DSR evaluation guidance [49] with the help of scenarios. One main simulated scenario of the organisation is defined, and the dashboard is populated with relevant simulated data, which is then interpreted with the five research questions (RQ1-RQ5) [50] to create the OSMI, domain profiles, RAG classifications and prioritised recommendations. The evaluation criteria applied are internal consistency, reproducibility, comparability and continuous improvement, which are all directly related to design requirements identified in Phase 1 and deficiencies identified in Chapter 2 from the literature. Analytical checks also assess the monotonicity and sensitivity of the scoring, which is important for the OSMI to be a governance tool, and not just an averaging artefact [51].

The evaluation process ends with a critical reflection on the strengths and weaknesses of the framework and dashboard and recognises that the evaluation is conceptual and has not been tested in live organisations [52]. Theoretical guidelines are then drawn to guide the organisations in how they could adopt the framework, fit the framework into their audit cycles for an existing ISMS and develop the prototype towards more sophisticated tooling [53]. This reflective step completes the traceability loop which was set up during Phase 1 and explicitly revisits each design requirement, and considers how well the final artefact meets it, with any gaps and trade-offs being clearly recorded and suggestions for future empirical validation provided [54].

3.5 Methods, Materials, and Tools

The methods used at the four phases are as follows: Literature synthesis and critical analysis for grounding and requirements; conceptual modelling for framework and scoring design; web-based implementation by HTML, CSS and JavaScript for dashboard instantiation, and conceptual evaluation and reflective analysis based on scenarios [55]. All of these approaches implement the DSR cycle in the context of a theoretical dissertation: the literature synthesis motivates and shapes the artefact; the conceptual modelling and web implementation builds and instantiates the artefact; and the scenario based evaluation and reflection, provides a structured ex-ante assessment of the artefact's utility and rigour [56]. The study only uses published ISO standards, academic articles and industry frameworks as documentary data and simulated assessment data in the form of hypothetical organisations, which means that there are no risks of using sensitive or real organisational data, and that ethical risks are minimised [57]. The software tools used are reference management software for managing citations, draw.io for making framework architecture and scoring flow diagrams and a normal web development environment (HTML/CSS/JavaScript with Chart.js) for the interactive dashboard prototype [58]. These tools are sufficient to support the conceptual design, implementation and documentation of the proposed framework in the technical and resource constraints of the project, and the use of widely available web technologies (open-standards) allows for the potential replication and initial piloting of the artefact in organisational settings without the need of special infrastructure [59]. The dissertations are prepared using standard word processing software, and all design decisions, scoring rules and framework parameters are described in enough detail to allow for independent research situations to be reproduced.

3.6 Ethical Considerations

There are two aspects of ethical issues in this research: Research Conduct Ethics and DSR-specific Artefact Ethics. In terms of conduct, this dissertation does not produce any primary data from human subjects, gather any personal or organizational information and does not use any experimental interventions – it is purely desk-based and artefact-constructive in nature [61]. [62] define a set of ethical principles that are specifically related to DSR in information systems, which are divided into four main principles: the welfare of affected parties, justice in the distribution of research benefits, respect for persons and transparency in artefact evaluation. In this dissertation, each of these criteria is met: there are no human participants in the research; the outputs of the research are intended to be public and can be used by other sectors of the organisation; the design rationale of the artefact is fully documented; and the limitations of the artefact, such as the lack of live empirical validation, are made transparent. The simulated data approach has the downside of not being able to generalise the evaluation results, but avoids the ethical problems of using confidential organisational security posture data [63].

The ethical requirement to make sure that the instrument designed does not mislead decision makers for governance is addressed at the DSR artefact level, through the analytical verification procedures described in Phase 4 – namely monotonicity and sensitivity checks that ensure that the OSMI reflects actual performance at the level of control and does not generate misleading aggregate values [64]. According to [65] the decisions about the use of artefacts involve implicit ethical responsibilities for their consequences, which are resolved in this instance by explicitly documenting the assumptions, weighting defaults and boundary conditions of the OSMI, so that practitioners are able to make informed decisions on the applicability of the artefact to their governance context. This means that the transition sentence from this chapter to chapter 4 is not only methodological justification, but also the specification of the design, the epistemological, strategic and procedural foundations laid out in this chapter are directly related to the architectural decisions made in chapter 4, including the five-level scale, domain structure, OSMI logic and dashboard implementation [66].

4 Framework Design, OSMI Architecture, and Dashboard

4.1 Introduction to the Framework Design

The artefact created in this research consists of three closely related layers: a conceptual maturity model based on ISO/IEC 27001:2022 Annex A, an OSMI scoring architecture that combines control-level scores to provide domain and enterprise-level scores, and a browser-based dashboard with HTML, CSS, JavaScript and Chart.js [67]. This multi-layered structure is a direct reaction to the gaps found in Chapter 2 where either the frameworks were only checklist based compliance or they did not have a single, communicable measure of organisational security maturity [68]. The artefact implements the requirement of design science that new models must be instantiated and testable, rather than conceptual, and thus allows for a rigorous ex-ante evaluation, based on simulation with scenarios [69] within a web-based dashboard. The rest of this chapter provides more detail for each architectural layer in turn, providing clear traceability to Annex A and the design requirements listed in the Phase 1 traceability matrix

4.2 ISO/IEC 27001:2022 Annex A Domain Architecture

The control landscape has been restructured into the four thematic areas of Organisational, People, Physical and Technological in accordance with the intention of the ISO/IEC 27001:2022 committee to move away from lists of clauses and towards governance-based groupings of controls [73]. The four-domain architecture is carried over from the maturity framework without change since this allows for direct interpretability within the existing ISMS architecture and can be used as a filter in the attribute-based view used by ISO/IEC 27002:2022 for the security domain, operational capability, and cybersecurity concept [74]

In this context, Annex A controls are categorized as Organisational controls, People controls, Physical controls and Technological controls [76] respectively. This grouping is analogous to the one used in the current maturity and benchmarking methods, which allow organisations to identify asymmetries, e.g., good technology controls, but weak people or physical controls [77]. The choice to use the domain structure of the framework as found in Annex A and not other taxonomies, therefore, provides a basis for the artefact to be aligned to the de facto global

standard, and also allows cross-mapping to NIST CSF 2.0 functions and implementation tiers if desired [78]. Thus the domain architecture serves as a structure constraint and an enabler that ensures that all the elements of the OSMI are understandable in terms of recognised standard categories.

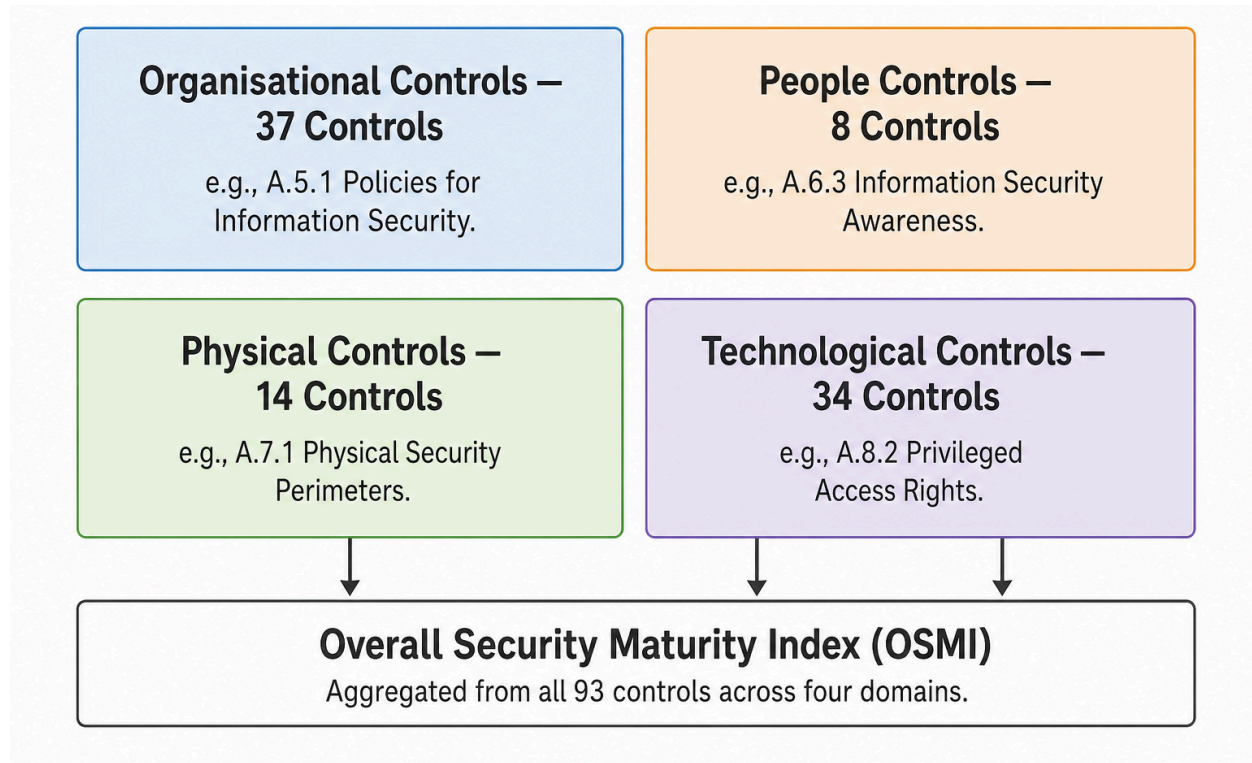


Figure 4.2 : Summary of 4 Domain

4.3 The Five-Level Maturity Model

The framework uses a five-level maturity scale ranging from Level 1 (Ad-hoc) to Level 5 (Optimising) where each level represents a greater level of process standardisation, integration, measurement and continuous improvement [79]. The five-level progression is intentionally designed to be at the same level of granularity as capability maturity models like the CMMI v2.0 which have proven that five levels offer adequate granularity to differentiate meaningful capability differences while maintaining a manageable complexity for assessors [80]. There is a de facto standard for five-level scales in ISO 27001-aligned maturity models and sector-specific

cyber maturity frameworks, which further supports the use of five-level scales for comparability and interpretability as shown by [81].

Each level is clearly described by observable indicators, which are common to all Annex A controls, allowing for maturity assessment based upon evidence and not impression [82]. At level 1 (Ad-hoc), control activities are performed informally, inconsistently and without documentation. Level 2 (Repeatable) indicates that practices are consistent but not documented or locally documented and are initiated by team and/or individual. Level 3 (Defined) is a level where procedures are formally documented and are part of organisational processes. Level 4 (Managed) requires systematic monitoring, measurement and review of the effectiveness of controls, and Level 5 (Optimising) requires continuous improvement that is based on metrics, learning from incidents and emerging threat intelligence [83]. These level descriptors are aligned with the level of maturity mentioned in the NIST CSF 2.0 tiers, and the good practice cybersecurity maturity guidance from ENISA, which moves from partial, risk-informed and repeatable practices to adaptive, intelligence-driven processes [84]. The scale thus serves as a link between the theoretical ideas of governance and the actual states of the implementation of the Annex A controls.

Table 4.3 : Five-Level Maturity Scale

Level	Label	Process State	Documentation Status	Measurement & Monitoring	Continuous Improvement	Example Indicator (Access Control)
1	Ad-hoc	Informal, inconsistent, reactive	None or ad hoc notes	None	None	User provisioning performed informally on request;

						no record kept
2	Repeatable	Consistent but undocumented; team/individual-dependent	Locally documented or informal	Informal observation only	None — reliant on individual skill	User provisioning follows a consistent manual routine; no formal workflow
3	Defined	Formally documented; integrated into organisational processes	Formally documented procedures exist	Periodic, rule-based checks	Ad hoc review following incidents	Provisioning procedures documented; workflows followed across teams
4	Managed	Systematic monitoring, measurement and review of control effectiveness	Documented with version control and review schedules	Regular, structured metrics collected	Scheduled improvement cycles based on metrics	Access reviews automated; periodic access certification performed

5	Optimising	Continuous improvement driven by metrics, incident learning, and threat intelligence	Living documentation updated via feedback loops	Real-time monitoring and intelligence-driven adaptation	Continuous, intelligence-driven	Behavioural analytics and adaptive access decisions based on threat intelligence
---	------------	--	---	---	---------------------------------	--

4.4 Control Assessment Indicators and Mapping Logic

The framework contains qualitative and quantitative indicators to differentiate the five maturity levels for each Annex A control, which overcomes the assessor subjectivity and reproducibility issues found in the literature. Common symptoms are the presence and up-to-date procedures, level of integration in business processes, assignment of responsibilities, evidence of training and awareness, implementation of technical measures, and monitoring, metrics and continuous improvement mechanisms [85]. For instance, in an access control context, Level 2 could be where user provisioning is consistently performed manually, Level 3 could be where the user provisioning procedures are documented in workflows, Level 4 could be where user provisioning is automated with regular access reviews, and Level 5 could be where behavioural analytics and adaptive access decisions are made based on threat intelligence [86]. The framework is grounded in observable conditions and this minimizes the interpretive ambiguity and ensures consistency in assessment of the levels across assessors and time points [87].

The indicator logic is not generic, but is clearly driven by the guidance of ISO/IEC 27002:2022 and current risk assessment and governance literature. [88] stress the importance of explicitly connecting control to risk scenarios to be effective in information security risk assessment and [89] stress the need to shift away from static risk matrices to dynamic control capability assessment. The indicators listed here directly address those observations by incorporating

control – risk linkage at each maturity level and the need for evidence of the presence of controls, and their effective embedding into risk management processes. Furthermore, sector-specific frameworks, like NIST SP 800-161 on supply chain risk and NIST SP 800-160 on systems security engineering, guide the design of the indicators in supplier security and resilience-related controls, providing maturity assessment with consideration of current supply chain and resilience challenges [90]. The mapping logic thus makes sure the maturity model isn't a generic overlay, but rather is a standards-aligned, risk-aware representation of Annex A implementation.

4.5 OSMI Scoring Model and Aggregation Rules

Existing frameworks do not have a structured aggregation mechanism, which is addressed by the OSMI scoring architecture that translates the maturity assessment at the control level to numeric values and aggregates them to domain-level scores and a single Overall Security Maturity Index (OSMI). A numeric score is assigned to each control according to its maturity level (usually 1–5) and these scores are added together within the domains using a transparent additive model based on Simple Additive Weighting (SAW), a widely-used method in multi-criteria decision analysis [91] [92]. Domain scores are calculated as simple or weighted averages of control scores, where weights are defaults and can be adjusted according to risk context and justified by organisations [93, 94] and the OSMI is calculated as a weighted average of the domain scores, also with defaults and optional organisation-specific weightings justified according to risk context. This structure maintains the interpretability but also allows organisations to focus on specific areas, such as giving more weight to Technological controls in cloud-native environments, or to People controls in highly regulated industries.

The scoring mechanism undergoes analytical testing for three important properties: monotonicity, boundedness and sensitivity, to ensure that the OSMI is a valid governance measure and not some mathematically convenient but misleading measure. The additive, non-negative weighting structure [91, 95] ensures monotonicity, which means that if a control-level score is improved the domain or overall score cannot be lowered. Boundedness helps to keep scores within a range, usually 1-5, by scaling both domain and OSMI values to the same range, which helps to maintain comparability across organisations and over time [96, 97].

Sensitivity means that a significant deficiency in one domain shouldn't be masked by high scores in other domains; this is done by limiting the weights and by graphically presenting the scores for each domain in addition to the OSMI score, so that the low-performing domains are always visible and cannot be obscured by the overall score [93, 94]. The resulting OSMI is therefore mathematically sound and relevant for governance, as it combines the desire to keep it as one communicable index with the necessity to not oversimplify it.

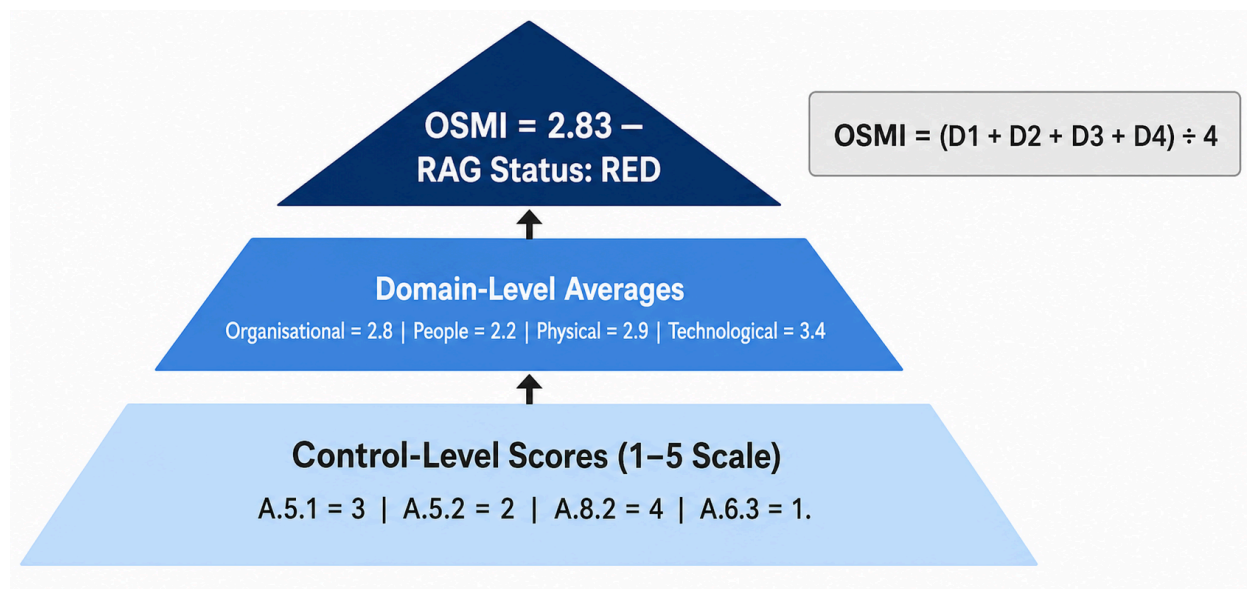


Figure 4.5 : OSMI Architecture

The OSMI logic also reflects the current trend in risk-based governance guidance that maturity scores should be used to prioritise and drive continuous improvement, and not be the end in themselves. Viking Cloud [98] point to the importance of metrics in risk-based security which show where the biggest risk reduction can be achieved by implementing security, and Zero Networks [97] note that benchmarking defences requires indices that measure the breadth and depth of defence implementation. This is exactly the kind of governance desired, and it is provided for directly by structuring the OSMI as a weighted domain-specific index and providing both overall and domain-specific scores [95, 99]. The scoring structure thus serves as the mathematical core of the artefact, and allows for a strict and repeatable maturity assessment in the landscape of Annex A.

4.6 RAG Status Classification and Prioritisation Logic

However, numeric maturity scores are not sufficient to lead to better decision-making; they need to be transformed into 'signals' that can be understood and can help non-specialist governance actors to prioritize rapidly. This requirement is addressed in the framework by a Red–Amber–Green (RAG) classification scheme both at control and domain level, where thresholds are tuned to make sure that the classification decision is sensitive to meaningful differences in maturity [1]. For instance, Level 1-2 can be considered as Red (high risk/low maturity of control posture), Level 3 as Amber (lowest acceptable level but with potential for improvement) and Levels 4-5 as Green (advanced/high maturity of control posture), with exact levels able to be customised to the risk appetite of the organisation [2]. The RAG statuses are the main visual indicators displayed on the dashboard and are used to quickly identify weak domains and controls even for those stakeholders who may not be involved with the numeric values themselves [3].

Table 4.6 : RAG Status Classification

RAG Status	Maturity Score Range	Maturity Level Label	Governance Interpretation	Prioritisation Class	Recommended Action
Red	1.0 – 2.49	Ad-hoc / Repeatable	High risk; control posture critically insufficient; no reliable governance mechanism in place	Immediate — Priority 1	Establish formal procedures; assign control ownership; initiate documentation programme
Amber	2.50 – 3.49	Defined	Minimum acceptable threshold reached; formalisation in	Medium — Priority 2	Introduce monitoring and metrics; integrate controls into

			place but measurement and adaptation absent		business process review cycles
Green	3.50 – 5.00	Managed / Optimising	Mature control posture; active governance, measurement and improvement evident	Sustain — Priority 3	Maintain current practices; document as internal benchmark; extend to lower-maturity domains
Unscore d	N/A	Not assessed	Control has not been evaluated; creates a blind spot in the OSMI calculation	Immediate — data completeness	Assign assessor responsibility; complete scoring before governance reporting

The prioritisation mechanism is tightly linked to the RAG logic, and provides suggestions for improvement based on the mix of maturity scores, domain weights and RAG classifications. Control or domains marked as Red are automatically identified as a high priority improvement target, especially if they are in a heavily weighted domain or have a risk scenario associated with them that is high impact, such as supply chain dependencies or incident response capabilities [4]. Elements classified as Amber are considered medium priority, recommendations include streamlining current processes, improving monitoring and measurement, and elements classified as Green are strengths to be retained and/or leveraged as internal benchmarks and/or exemplars [5]. This logic applies the continuous improvement and learning-from-incidents principles that are stressed in ISO/IEC 27005:2022 and in the current literature on incident learning, making the outputs of the dashboard not only descriptive, but also prescriptive and aligned to standards [6].

RAG and prioritisation design thus ensures that the outputs of the OSMI can be actioned within governance processes and are not just abstract scores, de-contextualised from decision making

5 Dashboard Implementation and Design Decisions

The dashboard implementation is the actualisation of the conceptual maturity framework and the OSMI scoring architecture into a tangible HTML/CSS/JavaScript artefact that users can interact with to evaluate the maturity of the Annex A controls and understand the results of the OSMI. The chapter looks at the important aspects of that implementation including the layout, scoring, visualisation, RAG status, and design trade-offs of the dashboard, and how all these elements combine to further the research aim of moving beyond checklist compliance towards strategic, maturity-informed governance. Every subsection discusses one architectural decision and shows how it implements the design requirements identified in Chapter 3 and helps to answer RQ3 and RQ4.

5.1 Introduction to Dashboard Implementation

This implementation decision directly contributes towards the goal of creating an accessible artefact that is standards compliant and can be deployed without proprietary tooling, and can still be visualised interactively at the domain level in terms of maturity and the OSMI [23]. Instantiating the maturity framework as a browser-based interface, instead of a static spreadsheet, satisfies the design science requirement of an evaluable artefact in a way that allows for ex-ante scenario-based evaluation and future extensibility [24]. The rest of this chapter examines how the structure and behavior of the dashboard was designed to retain the rigor of the underlying scoring model, while maximizing the interpretability and usability of the dashboard.

5.2 Front-End Architecture and Layout

The front-end architecture of the dashboard is divided into three sections: the header, the main content section (which has three panels: input, visualisation, recommendations) and the footer. The header includes the dashboard title, a short description of what the dashboard is used for, and a theme toggle to give quick orientation and accessibility with clear labelling and consistent navigation [25, 26]. The main content area is split into three sections: an input panel on the left to input control maturity levels; a visualisation panel in the middle to display OSMI and domain scores in charts; and a recommendation panel on the right to display RAG status and prioritised

actions [27], [28]. The design of this layout reflects the cognitive process through which users experience assessment workflows – from input to computation to visual insight to action – and highlights the dashboard as a decision-support tool, not just a reporting tool.

The layout is designed with CSS grid and flexbox, and responsive breakpoints are used to switch the three column layout to a stacked layout when the window is smaller, while maintaining the ordering [29] [30]. This design allows for the dashboard to be usable on both desktop and mobile devices, which is important since security governance tools must be able to handle a wide variety of usage scenarios, such as distributed teams and remote audits [31] [32]. Semantic sectioning elements and ARIA roles also help screen readers to navigate and are consistent with current accessibility and usability standards [33] [34]. All these design choices combine to make the dashboard structure facilitate the separation of concerns – data entry, data computation, and data interpretation – and keep it in line with the overall design principles presented in Chapter 4.

5.3 Input Layer: Control Scoring Interface

The input layer allows the assessor to use a structured interface to assign a maturity level to each of the Annex A controls, while maintaining a high level of detail and ease of use. The controls are listed in a well-structured table or list, each one with the control identifier, a short description, the domain (Annex A) and a dropdown to select the maturity level (1-5) according to the predefined indicators. This design has been implemented to limit user options to the appropriate levels and to give feedback to the assessor in the form of brief level descriptions or tooltips, to help them understand the criteria associated with each level [35, 36]. The interface directly responds to the issues of subjectivity and reproducibility of assessors in the literature [37], [38] by converting the qualitative indicators into structure input options.

Also, domain-based grouping in the input interface helps with cognitive alignment with the architecture of Annex A, and helps with the subsequent interpretation of domain level scores, as assessors can easily see which controls contribute to which domain's maturity profile [35], [39]. The interface also has simple validation features, such as only accepting valid numeric levels and requiring that mandatory controls for a given scenario be assessed, thus helping to ensure internal consistency of the scoring process [40], [41]. The overall impact of these design

decisions is that the input layer implements the control-level granularity of the framework, while also reducing the friction for assessors, to make the framework more feasible to adopt in real organizational contexts.

5.4 Scoring Engine: JavaScript OSMI Logic

The scoring engine is written in JavaScript and consists of a series of functions which transform input maturity levels into numbers, calculate domain averages and add them together to create the OSMI based on the Simple Additive Weighting logic defined in Chapter 4. The selected level for each control is translated to a numeric score, on a 1-5 scale and domain scores are computed as simple averages or weighted averages (where domain-specific weights are configured), allowing for both equal and risk-based weighting strategies [42], [43] to be used in the engine. The OSMI is then calculated as a weighted average of the domain scores; the weights are initially set to be equal and can be modified by the user, but interface cues and documentation keep the weights transparent to the users. The functions are intended to provide transparency and auditability, so that users and evaluators can see all intermediate and final values, and understand how each of the control scores contributes to the overall scores for each domain.

The scoring engine includes run-time validation checks to guarantee that the mathematical characteristics of monotonicity, boundedness and sensitivity are maintained. For instance, the engine checks that if an OSMI value is in the 1–5 range, and the control score is increased, the domain score and overall score do not decrease, which could otherwise lead to counter-intuitive results that would be difficult to trust [46, 44]. Sensitivity is achieved by limiting the ability to mask out domains with low scores with high scores in other domains (bounded weighting) and by the visual design of the dashboard, which always displays domain-level scores in addition to the OSMI [43, 47]. The implementation decisions are consistent with the DSR focus on internal artefact quality, and ensure that the scoring engine works predictably and sensibly on the simulated scenarios that are used to evaluate the system in Chapter 6 [48, 49]. The engine, therefore, serves as the computational engine to transform qualitative maturity assessments to strong, governance-relevant metrics

5.5 Visualisation Layer: Chart-Based Domain and OSMI Views

The visualisation layer is based on Chart.js and allows OSMI and domain-level scores to be presented as an interactive radar and bar chart, which allows intuitive interpretation of maturity profiles. Radar charts represent the four Annex A domains with their respective maturity scores, and give an instant visual impression of strengths and weaknesses in the four areas of organisational, people, physical and technological [50, 51]. This format is well suited to show domain asymmetries, such as high technological capability, but low people controls, that would otherwise only be apparent in numeric tables [52], [53]. Bar charts are used to complement the radar charts to display domain scores and the OSMI on a common scale and facilitate easy comparison between domains or scenarios and enhance the interpretability of the aggregated index [54,55].

The visualisation layer has been designed to be accessible and easy to understand: colour schemes are designed to match the RAG classification (e.g. red for low scoring domains, amber for medium and green for high), and each chart is annotated with text and numbers to support users who may not be able to interpret the visualisations alone [50], [56]. All charts are contained in responsive containers that fit to the size of the screen, and tooltips give more information on demand, including actual scores and explanations at the domain level [57] [58]. These design decisions make the charts the key instruments for boosting cybersecurity situational awareness, as they are able to convey complex security situations through both visual and textual means, which is supported by evidence that interactive dashboards can help with understanding complex security situations [59] [57]. The visualisation layer then translates the outputs of the scoring engine into visualisations that are easy to understand and use for comparison and that directly inform governance decision making.

5.6 RAG Status and Recommendation Panel Implementation

The RAG status and recommendation panel is a translation of the numeric scores to prioritised, governance-oriented guidance to help close the gap between measurement and action. The panel is fed with domain and control scores from the scoring engine and ascribes Red, Amber or Green statuses based on thresholds that are set by the organisation, as per their risk appetite, usually

with a score of Level 1-2 being classified as Red, Level 3 as Amber and Level 4-5 as Green [60,61]. These statuses appear next to each domain name and key controls, through colour coded badges and labels that use short phrases to help decision makers know at a glance which areas need to be addressed and which are satisfactory or exemplary [62] [63]. The panel design thus implements the RAG logic outlined in Chapter 4 and prevents the low maturities domains and controls being masked by the single overall value of the OSMI.

In addition to classification, the panel also provides text-based recommendations which are directly linked to the controls and maturity levels in Annex A, thus facilitating traceable and standards-based improvement plans [64, 65]. For instance, a Red rating in the People domain could lead to a recommendation to formalise security awareness training programmes and implement effectiveness measures, as evidence shows that targeted, maturity-aware training programmes can help to decrease human error related incidents [66] and [67]. Likewise, Amber statuses can be used to trigger consolidation activities like monitoring or periodic reviews, and Green statuses can be used to identify practices to maintain or use as internal benchmarks [68, 69]. This recommendation logic translates risk-based security guidance into actionable information, making sure that dashboard outputs not only tell organisations about their maturity, but also focus them on specific, prioritised actions that can help them get better in OSMI and security in general [61] [70].

6 Scenario-Based Evaluation and Interpretation of Dashboard Outputs

In this chapter, the proposed artefact is tested by simulating organisational scenarios, by generating domain maturity profiles, RAG status classifications, prioritised recommendations and Overall Security Maturity Index (OSMI) using the HTML/CSS/JavaScript dashboard. This is an ex-ante and artificial evaluation, as the dissertation is based on a theoretical Design Science Research approach, where utility and internal rigour are evaluated in a controlled scenario, and where the behaviour of the artefact in the controlled scenarios revisits RQ1-RQ3, while the chapter is central in answering RQ4 and RQ5. Therefore, the analysis does not aim for empirical validation, but rather to check the plausibility of the outputs of the framework and their interpretability and strategic usefulness, which addresses the limitations discussed in the previous chapters, especially the focus on checklist compliance, weak comparability and poor prioritisation support in existing ISO 27001-aligned approaches.

6.1 Evaluation approach and scenario logic

The evaluation strategy involves using the simulated maturity inputs on a representative subset of Annex A controls spread across the organisational, people, physical and technological domains and interpreting the scores for each of the domains, the OSMI and the visuals on the dashboard against the design requirements that were set out previously. This is in line with recent cybersecurity maturity work with a design focus, in which artefacts are tested using realistic but hypothetical organisational profiles that are used to analyse the internal consistency, comparability and value for decision support before field deployment is possible [83] [84]. The rationale behind the evaluation is therefore not statistical, but analytical: when the artefact is well designed, changes in control-level maturity should result in coherent changes in domain scores and in OSMI, weak aspects should not be masked by strong aspects, and the dashboard should help to make decisions about improvement; something that binary compliance checklists cannot do [85] and [86].

Scenario A is a medium sized service provider with medium regulatory pressure, medium technical investment, but low governance integration and behavioural reinforcement, which is a

typical organisational model where the pace of technology is outstripping the pace of governance integration and behavioural reinforcement [87, 88]. In Scenario B, a more compliance-focused, but operationally inconsistent organisation has more formalisation of policies and less continuous monitoring and optimisation, with limited feedback loops and risk-based adaptation [89, 90] still holding the organisation back. The scenarios were chosen as they directly challenge the dissertation's main argument that organisations frequently possess visible compliance artefacts, but fail to reach the state of security maturity, where security is balanced across the enterprise [91, 92].

6.2 Scenario A: Mid-sized service provider

The simulated control scores in Scenario A show a moderate level of maturity in the technological domain, a lower level of maturity in the organisational and people domains, and a low level of maturity in the physical security domain, resulting in an uneven maturity profile, which is clearly visible in both the numeric and visual outputs from the dashboard. A reasonable profile for this scenario would be Organisational = 2.6, People = 2.2, Physical = 2.8 and Technological = 3.4 which gives an OSMI of ~2.75 under equal weighting, putting the organisation in the top end of the Repeatable and not yet in a stable Defined maturity posture. This output is analytically relevant as it shows that the artefact does not mask weak governance and staff-related controls with an artificially high enterprise-wide rating: weaknesses are still evident and have a material impact on the enterprise-wide rating, which is the desired behavior to avoid the masking effects discussed in the literature on maturity aggregation [93] [94].

The dashboard interpretation for Scenario A is strategically important as the radar and bar views clearly indicate that people and governance gaps are more of a limitation than technology capability on its own can overcome in enterprise maturity. This finding reinforces the argument presented in Chapter 2 that compliance-based strategies often focus on the presence of documentary and/or technical controls, and not on behavioural and governance factors that are likely to affect whether controls are maintained and enhanced over time [95] and [96]. The practical implementation of the dashboard would result in the People domain being categorised as Red, the Organisational domain as Amber-Red boundary, the Physical domain as Amber and the Technological domain as Amber-Green boundary, and a sequence of recommendations would

be generated that would focus on awareness, accountability, policy integration and governance review before any further technical extension. The output thus reinforces the idea of the framework that maturity assessment should focus on structural imbalance, and not just on reinforcing the known controls in place [97] [98].

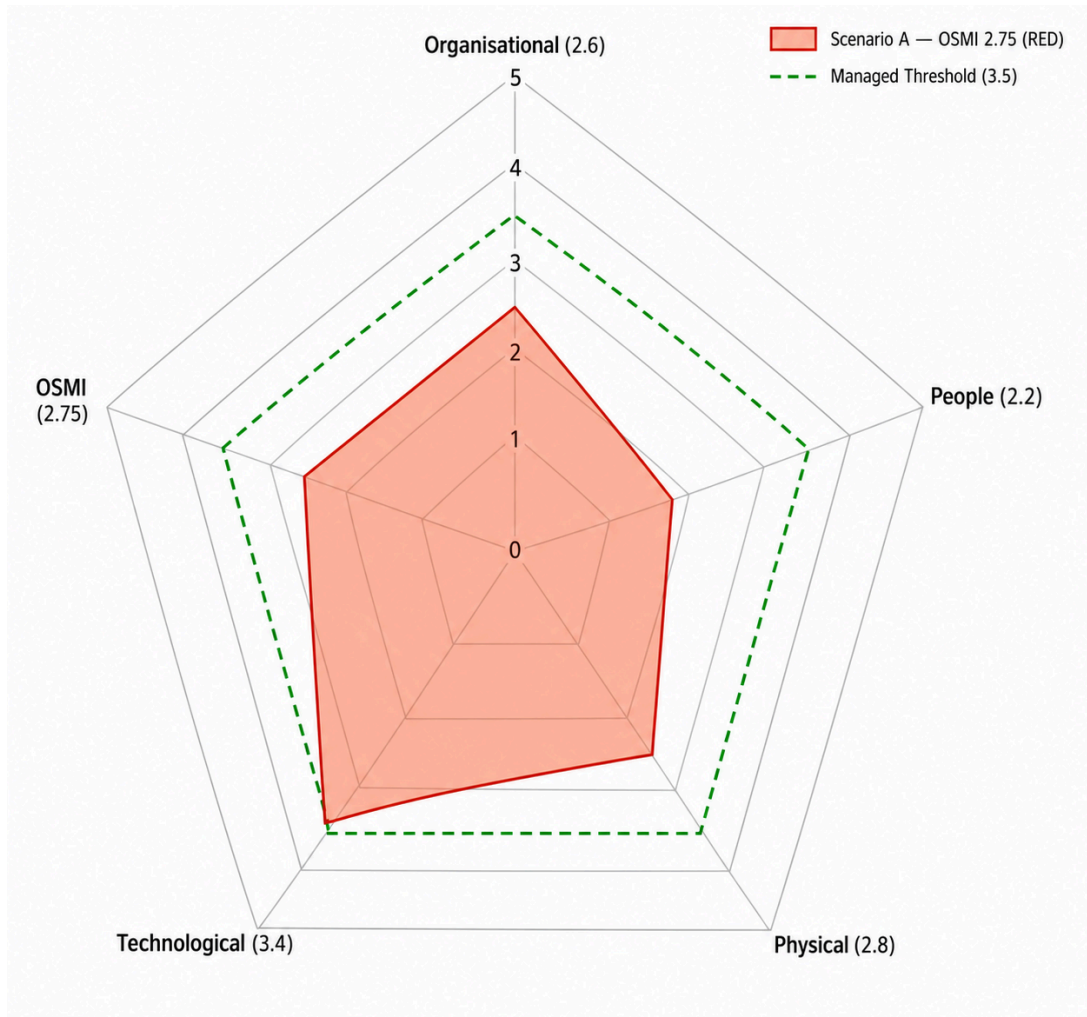


Figure 6.2 : Domain Maturity Tracker

6.3 Scenario A and research question alignment

Operational aspects of the limitations of frameworks that see ISO 27001 implementation as a compliance checklist are shown in scenario A, making it a direct response to RQ1. An organisation with such a state of affairs could be classified as broadly compliant by a binary or clause-complete assessment, if the core policies, access controls and selected safeguards were

present, but the maturity dashboard indicates that people practices were fragmented and governance mechanisms were underdeveloped, so that access controls were not being used as an integrated strategic system [20, 21]. The importance of this distinction lies in the fact that whilst conventional assessment modes are able to determine if a control is in place, maturity evaluation is able to determine how well a control is embedded, measured and improved over time [22], [23]

The same scenario also applies to RQ2 and RQ4 as it shows how intelligence can be gathered from a five-level maturity structure and OSMI and RAG outputs, and is more actionable than a set of non-aggregated compliance records. The domain scores provide insights into the areas of weakness, the OSMI provides insights into the organisation's overall position on a common scale and the recommendation layer provides a combination of measurement and governance guidance to improve the organisation's position – based on the patterns – into a set of improvement priorities [24, 25].

6.4 Scenario B: Formalised but uneven organisation

In scenario B, the focus is on a different organisational pattern, which is characterised by higher formal documentation of governance processes and a higher level of visibility of compliance structures, but lower monitoring, measurement and optimisation behaviour, particularly in technology assurance and continuous improvement processes. One reasonable set of outputs is Organisational = 3.5, People = 3.1, Physical = 3.0 and Technological = 2.7, which will give rise to an OSMI of about 3.08 and put the organisation at the bottom end of Defined maturity. Although this looks more mature than Scenario A, the dashboard indicates that the organisation's maturity is still fragile as managed and optimising characteristics are not in balance; in particular, operational monitoring and feedback should enable the organisation to move from formal compliance to adaptive security capability [28] [29].

This is a critical situation because it represents another compliance trap – one in which compliance is demonstrated by having the structures in place, but not necessarily by having the effectiveness measured and the control process improved. It is repeatedly mentioned in literature on implementation of ISO 27001 that formalisation of a policy can give the impression that the

security has been improved, although the assurance, learning from incidents and risk-based adaptation are not developed, so that the system is mature on the administrative level, but brittle on the operational level [30],[31]. The dashboard does not suffer from this issue as it does not summarise all documented activity into a positive maturity - it separates between Defined and Managed maturity - and therefore the Amber classifications in technological and optimisation-related areas indicate where formalisation has not yet become formalised active control governance. This validates the five-level structure's granularity to distinguish between the real maturity progression and static completeness of compliance answers to RQ2 [32, 33].

6.5 Comparative interpretation of scenarios

If Scenario A and Scenario B are compared, then the analytical value of domain level aggregation is made more apparent than either of the scenarios alone. They are differentiated by the OSMI but the domain profiles provide an explanation as to why they are different and what each organisation needs to do next to improve. This comparative feature directly tackles the comparability requirement defined in the methodology, which allows the cross-scenario benchmarking without eliminating the differences in maturity composition in a structure [42,43]. That is, the artefact enables to compare without oversimplification, one of the main gaps in design identified in existing risk assessment and maturity approaches [44] [45].

The comparative evaluation also helps in the validation of the practical logic of the framework, which is possible with the simulated outputs even without field deployment, as mentioned in RQ5. A useful artefact should not only produce numbers but numbers which act persuasively in the face of real-world organisational asymmetry: both scenarios demonstrate that the dashboard reacts in ways that are in line with current conceptions of cybersecurity capability, dependency on governance, and continuous improvement [46, 47]. The simulation offers a defensible form of conceptual validation within the scope of theoretical boundaries of this dissertation as the outputs are still interpretable and sensitive to weak areas and are aligned to the structural domains of Annex A. The scenarios thus serve not as an empirical evaluation, but as evidence of the internal consistency of the logic of the framework and the decision-relevance of the outputs.

Table 6.5 — Cross-Scenario Analysis

Domain / Metric	Scenario A: Mid-Sized Service Provider	RAG Status (A)	Scenario B: Formalised but Uneven Organisation	RAG Status (B)	Delta (B – A)	Governance Implication
Organisational Controls	2.6	Red	3.5	Green	+0.9	Scenario B has formalised governance structures; Scenario A lacks policy integration
People Controls	2.2	Red	3.1	Amber	+0.9	Both scenarios reveal under-investment in security culture and awareness capability
Physical Controls	2.8	Red	3.0	Amber	+0.2	Physical domain is weak across both scenarios; warrants prioritised remediation
Technological Controls	3.4	Green	2.7	Red	–0.7	Scenario B's formalisation masks weak technology assurance and monitoring practices
OSMI (Equal Weighting)	2.75	Red	3.08	Amber	+0.33	Scenario B is marginally more mature overall but operationally fragile in technology

Maturity Band	Repeatable (upper boundary)	—	Defined (lower boundary)	—	—	Neither scenario achieves Managed maturity; both require structured improvement planning
---------------	-----------------------------	---	--------------------------	---	---	--

7 Discussion, Limitations and Future Research

This chapter brings together the dissertation's contribution by evaluating the degree of accomplishment of the dissertation's aim and objectives, identifying some of the key limitations of the proposed framework and dashboard and identifying a focused agenda for future research. The chapter is important because the usefulness of a Design Science Research artefact is not just determined by buildability, but by how the conceptual logic, evaluative performance and positioning combine to establish the relevance of the artefact to the problem as stated, which in this case is the continued use of ISO/IEC 27001 as a compliance checklist versus a strategic tool for enterprise-wide maturity improvement. The discussion thus returns to the study's contribution in view of the scenario-based evaluation, but keeping a critical attitude towards the scope of the scenario, the assumptions and the evidential limits of the scenario, which is very important for a rigorous level 7 dissertation.

7.1 Achievement of the research aim

The research goal was to create and implement an interactive tool that would allow organisations to assess how well they are implementing the ISO/IEC 27001 Annex A controls on a five level maturity scale and generate an Overall Security Maturity Index (OSMI). This goal has been achieved at the conceptual level and proof of concept by creating an Annex A aligned maturity framework, a structured scoring logic, a domain based aggregation model and by creating a browser-based dashboard that can display organisational maturity profiles and prioritised outputs for improvement. What is important is not only the creation of a dashboard, but the development of a coherent artefact that connects the control level evidence, domain level interpretation, and enterprise level maturity representation in a manner that is not usually done in the traditional ISO 27001 compliance assessments (Proenca and Borbinha, 2020; Ozkan et al., 2021). In this regard, the artefact provides a practical and theoretical solution to the lack of strategic security governance and formal certification activity for a long time.

The research aim has also been achieved on a methodological level as the artefact is not just a purely technical product, but a designed solution to a problem space that has been well defined. The study used a critical literature synthesis as its basis for developing the requirements, translating the identified deficiencies into formal requirements for the artefact, and analysis of the artefact in the context of scenarios, which followed the logic of ex-ante DSR. This is essential as it is not possible to reduce the contribution to a software prototype: the framework represents a set of design principles concerning the measurement of maturity, comparability, prioritisation and governance alignment that go beyond the interface. The result obtained is therefore best thought of as a maturity assessment artefact which is structured and represented as a dashboard instantiation, rather than as an enterprise product and this distinction highlights the strengths and the limitations.

7.2 Achievement of the research objectives

The aim of Objective 1 was to find out what is missing from current maturity models and risk assessments for organisations to progress beyond the checklist approach. This objective was accomplished by conducting a literature review and a subsequent problem grounding, which revealed that many approaches based on ISO 27001 still focus on the presence of the controls, the inconsistent assessor judgement, the lack of cross domain comparability and the lack of support for prioritised improvement, even if the formal compliance processes are well developed. The study concluded that these deficiencies were not incidental and that there was a need for a framework that could consider Annex A controls as maturity variables as opposed to just pass/fail checkpoints. This objective was therefore the analytical basis on which the latter design work was based.

Objective 2 needed to justify a DSR approach to developing a practical tool which can be aligned to ISO 27001. This was done by being artefact oriented, problem oriented and theory oriented, which was appropriate for the goal of developing a maturity model and dashboard, rather than testing an existing theory, using primary data collected in the field. The adopted DSR logic facilitated the research to progress from requirements derived from literature to the conceptual

design, dashboard implementation, and scenario-based evaluation, which in turn, illustrated the methodological fit between the research problem and the mode of inquiry. The study did not therefore simply take DSR as a methodological label but it structured the production and evaluation of a purposeful artefact to intervene in a practical governance problem using DSR.

Objective 3 was to map the controls in Annex A to four domains and create a five-level maturity scale and generate an OSMI. This objective was realised in Chapter 4 and 5 by formally defining the domains (organisational, people, physical and technological), operationalising the maturity levels (Ad-hoc to Optimising) and developing an additive scoring model which converted maturity at the control level to scores for each domain and an overall index. This is important because it offers an enterprise-level maturity intelligence that is repeatable and traceable to Annex A that is missing from many existing ISO 27001 assessments based on distributed control observations. In this context the OSMI is not a stand-alone measure, but the end result of a carefully-designed domain-based maturity architecture.

As part of Objective 4, an interactive dashboard to score controls, visualise domain profiles and provide prioritised improvement guidance was developed. This was achieved by designing and discussing the HTML/CSS/JavaScript based dashboard that included input controls, a JavaScript based scoring engine, Chart.js visualisations and RAG based recommendation panels. The value of the dashboard is that it helps to visualize and make sense of maturity, as otherwise the framework would be abstract and inaccessible to the governance stakeholders. The dashboard thus was both an artefact and a tool that enabled the maturity, prioritisation and cross-domain imbalance to be made actionable.

Objective 5 involved testing of outputs with simulated scenarios of interpreting OSMI, RAG status and recommendations. This was realised in Chapter 6 by comparing the two different hypothetical organisational profiles and checking the plausibility of the results of the dashboard, the differentiability of the results, and whether the results were relevant for decision-making.

Conceptual utility of the artefact was demonstrated in the evaluation as it was found that it could identify weak points, maintain domain visibility after aggregation and provide domain-specific improvement suggestions. Thus, all five objectives were achieved in the context of a theoretical DSR dissertation, but only to a conceptual level of validation and this has implications for the interpretation.

7.3 Contribution to the research questions

The study has been coherent in terms of the research questions (RQ1 to RQ5) as each research question represents a different phase in the artefact's development and evaluation. RQ1: What are the gaps in the current frameworks that prevent organisations from using a more holistic approach that goes beyond compliance? The answer to this question emerged from the literature review and was found to be that many current models do not provide a structured maturity scaling, do not have cross domain aggregation, do not prioritise strategically, and do not integrate Annex A controls with governance decision making. RQ2 was whether it would be possible to create a five-level framework and OSMI for all Annex A domains, which was addressed by the four domains model, level descriptors and transparent aggregation logic of the study. These are important contributions as they indicate that the artefact was not a collection of unconnected parts but developed from a series of design actions, which were analytically connected to the gaps identified.

RQ3 questioned the rationale behind building a dashboard based on ISO 27001 and the dissertation addressed this by considering the dashboard as an artefact instantiation that could support the conceptual design to be made operational, evaluated and communicated. RQ4 was how effective the dashboard is in identifying weaknesses and recommending improvements, and the scenario-based outputs revealed the dashboard could identify structural imbalances, maintain visibility across the domains, and provide differentiated recommendations based on the maturity level, instead of generic compliance recommendations. RQ5 sought to understand how simulated outputs validate the practical utility, standards alignment and interpretability within the bounds of ex-ante theoretical validation, and the Chapter 6 evaluation showed that simulated scenarios are adequate to test internal coherence, comparability and interpretability within the scope of ex-ante theoretical validation. The combination of problem diagnosis, framework design,

dashboard instantiation and analytical evaluation, as presented in the dissertation, in a single standards-aligned maturity artefact, is the greatest contribution of the dissertation.

7.4 Theoretical and practical significance

The study is of theoretical interest because it adds to the growing stream of research which aims to shift the paradigm of information security management from a compliance-based one to a dynamic capability and governance one. Specifically, it demonstrates how controls in ISO 27001 can be translated into maturity-bearing variables which are spread across governance-relevant domains, thereby bridging the gap between the standards literature and the design of a maturity model and the use of dashboards for decision support. This is relevant, as ISO 27001 scholarship has tended to focus on the benefits of implementation, the problems of certification or interpretation of controls, but less on how the standard could be implemented as a structured measurement and strategic prioritisation system, as opposed to being merely an audit framework. The dissertation thus offers a synthesis of standard structure, maturity logic and governance interpretation, which is design-oriented.

The study is also practically relevant as the artefact is designed to be "lightweight" and easily understood by the organisation, and to be easily adaptable to the organisation without the need for specialist infrastructure. A browser based dashboard that is based on common logic, common visual formats, and transparent calculations is more likely to be adopted in preliminary governance or internal assessment settings than a very complex analytical system that requires advanced tooling and/or specialist analysts. Furthermore, the adoption of Annex A domains maintains a familiarity of the organisations which can make adoption easier, as there is no need to remove ISO 27001 language to achieve maturity improvement. The significance is therefore not that the artefact is completely deployment ready, but that it provides an example of how a path forward to the use of maturity analytics in governance practice by standards-aligned organisations could be developed.

7.5 Limitations of the study

The most significant limitation of the study is that the evaluation is still conceptual and scenario-based and the artefact has not yet been directly tested in a live organisational context, for its practical usefulness. While this is methodologically sound for a Level 7 DSR dissertation, it does limit the conclusions that can be drawn with regards to the usability, assessor behaviour, organisational acceptance or impact on real world decisions. While simulated scenarios may illustrate internal logic and plausible behaviours, they cannot fully convey the messiness of the organisational politics, incomplete evidence, conflicting interpretations of stakeholders, or varying audit maturity that can be found in real ISMS situations. The findings should thus be seen as an indication of conceptual feasibility and not proven effectiveness in the field.

The second limitation is with respect to control coverage and granularity. While the framework conceptually covers all the Annex A domains, the prototype evaluation is based on representative control sets and simulated maturity assignments, and not on the comprehensive evaluation of all 93 controls in an actual organisation. This was required to maintain the analytical clarity and feasibility in the scope of the dissertation but it means the scalability, performance and interpretability of the framework under full-control operational conditions remains to be demonstrated. In this regard, some control domains might need more context-specific indicators than others, particularly if a sector is regulated in some way, is heavily reliant on cloud services, has a complex supply chain or has cyber-physical integration that significantly affects the practical manifestation of maturity. The artefact, therefore, provides a solid overall framework, rather than an industry-specific calibration.

The third is the model of the scoring. The additive aggregation logic and optional weighting approach were chosen for its maximal transparency and interpretability, but it does, of course, simplify the complex interdependencies that exist between security controls, governance structures and threat conditions. In reality, the maturation of one control can be significantly influenced by the maturity of other related controls and linearly aggregated maturation values do not necessarily reflect the true organisational security posture. The dissertation explored this deficiency in some ways with sensitivity logic and visible domain level outputs, but the model does not make any attempt at advanced dependency modelling, probabilistic reasoning or

dynamic threat adaptation and such should not be interpreted as a shortcoming of the model but rather a design choice for clarity.

7.6 Future research directions

The next big question is not one of conceptual coherence of the artefact, but how it fares in actual use by practitioners with real evidence, time pressures and governance responsibilities; this should be the next step in future research. The researchers could test the assessor consistency, usability, interpretive value and impact on improvement by using case studies, in organisations with various levels of maturity with ISO 27001, and expert panels or Delphi style reviews could be used to fine-tune the maturity indicators and assumptions of weighting in the framework. This would directly enhance the conceptual to practical validation of the OSMI and give the evidence base to assess its ability to be used as a management indicator, as opposed to a prototype construct. This is the one extension that is most crucial to progress the artefact towards practical adoption.

While the current version is a lightweight prototype using the browser, future versions will include the ability to upload evidence, audit trails, trend analysis over time, benchmarking between business units, scenario libraries, API integration with governance tools, and other more sophisticated analytics, including dependency-aware scoring and predictive improvement modelling. These developments would make the artefact more rich in terms of its operation, but would also need to be carefully governed to ensure transparency and avoid the dashboard becoming opaque or too complex for non-specialist decision makers. The focus of future research should therefore be on considering technical sophistication and interpretability of governance as a design tension, and not necessarily viewing more analytical complexity as necessarily being better for a maturity tool.

8 Personal Reflection

Deliberate sequencing, not effort, was one of the most important things I learned from this dissertation in order to manage my time well. At the start of the project, I considered reading, drafting, and editing to be a linear process, and thus had to rush to finish the chapters, as one chapter was dependent upon decisions made in previous chapters. I got more disciplined by breaking things down into smaller chunks, making weekly targets and having different time blocks for different activities. This helped to enhance efficiency and coherence of writing. I also found out how to plan more realistically by having inbuilt deadlines before submitting and prioritizing the most important tasks first. Learning that postgraduate writing involves checking arguments, verifying evidence and aligning the structure meant that I could not take for granted that I would be able to write a first draft and leave it at that.

My study skills were greatly enhanced as I learned to read more critically, with a purpose. Instead of pointing and noting about the sources independently, I started reading against specific questions, e.g. is it about compliance limitations, maturity modelling or governance integration. This altered my note making from summarising a lot to making notes of the main points of each source, how it was relevant to the research question and what it links to other literature. My writing was also improved as I realised that each paragraph should have a point, supporting evidence, analysis and linkage into the next paragraph. I no longer wrote about frameworks and began writing about why the limitations of the frameworks were a good reason to create a new artefact, and became more succinct and focussed.

The dissertation also helped to improve my skills in solving problems on my own which are multi-layered and complex. I learned to stop and go back to the central purpose and goals, and research questions, when I couldn't see the next step; to not write blindly. This avoided unnecessary deviation and helped me to keep track of things as I went through the chapters. It helped to break down large tasks into smaller pieces – conceptual design, implementation, evaluation criteria, interpretation etc. – and helped to organise and boost my confidence. This experience has overall been a lesson in consistency, control and reflection, as opposed to speed, when it comes to academic work. These are all skills of realistic planning, critical reading,

iterative writing and independent problem solving that I will take with me to the future academic and professional environments.

9 References

1. Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021) 'The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda', *The TQM Journal*, 33(7), pp. 76–105. Available at: <https://doi.org/10.1108/TQM-09-2020-0202>
2. International Organization for Standardization (2022) ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO.
3. International Organization for Standardization (2022) ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO.
4. Calder, A. (2022) ISO 27001/ISO 27002: A Pocket Guide. 3rd edn. Ely: IT Governance Publishing.
5. ISACA (2024) 'Navigating the ISO/IEC 27001:2022 transition: a 90-day challenge', *ISACA Journal*, 3. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2024/volume-3/navigating-the-iso-iec-27001-2022-transition-a-90-day-challenge> (Accessed: 3 May 2025).
6. National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: NIST. Available at: <https://doi.org/10.6028/NIST.CSWP.29> (Accessed: 14 April 2025).
7. Wangen, G., Hallstensen, C. and Snekkenes, E. (2022) 'Information security risk assessment: a systematic literature review categorising frameworks, methods, and models', *Journal of Information Systems and e-Business Management*, 20(1), pp. 1–42.

8. Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2020) 'Taxonomy of information security risk assessment', *Computers and Security*, 57, pp. 14–30. Available at: <https://doi.org/10.1016/j.cose.2015.11.001>
9. Lund, M.S., Solhaug, B. and Stolen, K. (2022) 'Dynamic risk assessment in cybersecurity: a systematic literature review', *Computers and Security*, 115, p. 102632.
10. Topa, I. and Karyda, M. (2021) 'From theory to practice: guidelines for enhancing information security management', *Information and Computer Security*, 31(1), pp. 59–81. Available at: <https://doi.org/10.1108/ICS-10-2021-0155>
11. Ghadge, A., Weiß, M., Caldwell, N.D. and Bourlakis, M. (2020) 'A systematic review of IT security risk management for supply chain', *Supply Chain Management: An International Journal*, 25(5), pp. 585–600.
12. Woods, D. and Simpson, A. (2022) 'SoK: a framework for asset-centric analysis of security posture', *Computers and Security*, 114, p. 102585. Available at: <https://doi.org/10.1016/j.cose.2021.102585>
13. Alali, M., Almogren, A., Hassan, M.M., Gardezi, A.R. and Alamri, A. (2021) 'Improving risk assessment model of cyber security using fuzzy logic inference system', *Computers and Security*, 74, pp. 323–339.
14. Georgiadou, A., Mouzakis, S. and Askounis, D. (2022) 'Detecting insider threat via a cyber-security culture framework', *Journal of Computer Information Systems*, 63(1), pp. 1–12.
15. Disterer, G. (2021) 'ISO/IEC 27000, 27001 and 27002 for information security management', *Journal of Information Security*, 12(2), pp. 92–100.

16. Susanto, H. and Almunawar, M.N. (2022) 'Managing compliance with an information security management standard', in Encyclopedia of Information Science and Technology. 5th edn. Hershey: IGI Global, pp. 1–14.
17. Alotaibi, M.J. (2023) 'Improvement of information security management by implementation of ISO/IEC 27001', International Journal of Computer Applications, 182(50), pp. 1–7.
18. Ahmad, Z., Ong, T.S., Liew, T.H. and Norhashim, M. (2021) 'Security monitoring and information security assurance behaviour among employees: an empirical analysis', Information, 12(7), p. 271.
19. Tanaka, H. and Tateishi, R. (2023) 'Evaluating the role of ISO/IEC 27001 controls in reducing information security incidents in enterprises', Journal of Cybersecurity and Privacy, 3(1), pp. 45–62.
20. GRC Solutions (2025) ISO/IEC 27001:2022 and ISO/IEC 27002:2022 — key changes and implementation. Available at: <https://grcsolutions.io/iso27001-and-iso27002-2022-updates/> (Accessed: 19 April 2025).
21. ISACA (2023) CMMI v2.0 — Capability Maturity Model Integration. Pittsburgh: CMMI Institute/ISACA. Available at: <https://cmminstitute.com> (Accessed: 7 May 2025).
22. Spruit, M. and Roeling, M. (2020) 'ISFAM: the information security focus area maturity model', in Proceedings of the 28th European Conference on Information Systems (ECIS). Available at: https://aisel.aisnet.org/ecis2020_rp/21 (Accessed: 2 April 2025).
23. Tariq, N. (2021) 'Towards information security metrics framework for cloud computing', International Journal of Grid and Utility Computing, 12(1), pp. 1–16.

24. Ozkan, B.Y., Spruit, M., Wondolleck, R. and Blesgraaf, J. (2021) 'The next step in cyber security maturity for organisations: a dynamic capability-based framework', *Journal of Cybersecurity and Privacy*, 1(4), pp. 585–599. Available at: <https://doi.org/10.3390/jcp1040030>
25. Almeida, F., Santos, J.D. and Monteiro, J.A. (2020) 'The challenges and opportunities in the digitalization of companies in a post-COVID-19 world', *IEEE Engineering Management Review*, 48(3), pp. 97–103.
26. Security Compass (2025) What are the NIST CSF maturity levels? Available at: <https://www.securitycompass.com/blog/nist-csf-maturity-levels/> (Accessed: 11 April 2025).
27. Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2021) 'Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Computers and Security*, 105, p. 102248.
28. Ponsard, C., Grandclaudon, J. and Bal, G. (2021) 'Guidance and tool support for the cybersecurity maturity assessment of SMEs', in *Proceedings of the 7th International Conference on Information Systems Security and Privacy*. SCITEPRESS, pp. 469–476.
29. Proenca, D. and Borbinha, J. (2020) 'Information security management systems — a maturity model based on ISO/IEC 27001', in *Business Information Systems, Lecture Notes in Business Information Processing*. Cham: Springer, pp. 1–14.
30. Domínguez-Dorado, M., Carmona-Murillo, J., Cortés-Polo, D. and Rodríguez-Pérez, F.J. (2023) 'Cybersecurity maturity model for smart grid critical infrastructure organisations', *Applied Sciences*, 13(12), p. 7316. Available at: <https://doi.org/10.3390/app13127316>

31. Al-Mayahi, I. and Mansoor, S. (2021) 'Information security maturity model assessment: empirical study on higher education institutions', *International Journal of Advanced Computer Science and Applications*, 12(3), pp. 340–351.
32. Kure, H.I., Islam, S. and Razzaque, M.A. (2022) 'An integrated cybersecurity risk management approach for a cyber-physical system', *Applied Sciences*, 12(12), p. 6108. Available at: <https://doi.org/10.3390/app12126108>
33. Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007) 'A design science research methodology for information systems research', *Journal of Management Information Systems*, 24(3), pp. 45–77. Available at: <https://doi.org/10.2753/MIS0742-1222240302>
34. Gregor, S. and Hevner, A.R. (2013) 'Positioning and presenting design science research for maximum impact', *MIS Quarterly*, 37(2), pp. 337–355. Available at: <https://aisel.aisnet.org/misq/vol37/iss2/3/> (Accessed: 28 April 2025).
35. Hevner, A.R. and Chatterjee, S. (2021) *Design Research in Information Systems: Theory and Practice*. 2nd edn. New York: Springer.
36. vom Brocke, J. and Maedche, A. (2019) 'The DSR grid: six core dimensions for effectively planning and communicating design science research projects', *Electronic Markets*, 29(3), pp. 379–385. Available at: <https://doi.org/10.1007/s12525-019-00358-7>
37. Saunders, M.N.K., Lewis, P. and Thornhill, A. (2019) *Research Methods for Business Students*. 8th edn. Harlow: Pearson Education.
38. Creswell, J.W. and Creswell, J.D. (2022) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 6th edn. Los Angeles: SAGE Publications.

39. Bryman, A. (2016) *Social Research Methods*. 5th edn. Oxford: Oxford University Press.
40. Park, Y.S., Konge, L. and Artino, A.R. (2020) 'The positivism paradigm of research', *Academic Medicine*, 95(5), pp. 690–694. Available at: <https://doi.org/10.1097/ACM.0000000000003093>
41. Ryan, G. (2022) 'Introduction to positivism, interpretivism and critical theory', *Nurse Researcher*, 25(4), pp. 41–49.
42. Wieringa, R. (2022) 'What is design science research?', in *Handbook of Research Methods for IS Value Creation*. Cham: Springer, pp. 35–60.
43. Recker, J. (2021) *Scientific Research in Information Systems: A Beginner's Guide*. 2nd edn. Berlin: Springer.
44. Nature Portfolio (2026) 'Philosophical stances in information systems research: a case analysis and critical reflection', *Humanities and Social Sciences Communications*, 13(1). Available at: <https://www.nature.com/articles/s41599-025-06427-x> (Accessed: 20 May 2025).
45. Jouini, M. and Rabai, L.B. (2020) 'Comparative study of information security risk assessment models', in *Innovations in Smart Cities and Applications*. Cham: Springer, pp. 475–484.
46. Beckers, K. and Pape, S. (2021) 'A structured CISO-tool for detecting social engineering attack scenarios', in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Cham: Springer, pp. 117–130.
47. ICT Institute (2024) *ISO 27002:2022 explained — physical controls*. Available at: <https://ictinstitute.nl/iso270022022-explained-physical-controls/> (Accessed: 6 April 2025).

2025).

48. Ngo, Q.T., Tran, H.T. and Nguyen, T.D. (2021) 'A scoring mechanism for evaluating cyber maturity across organisational controls', *Journal of Information Security and Applications*, 60, p. 102879.
49. Onwubiko, C. (2020) 'Cyber situation awareness: modelling the security operations centre', *Journal of Cybersecurity and Privacy*, 1(1), pp. 1–27.
50. Rodrigues, C., Araújo, J. and Basto, R. (2023) 'Applying design science research to develop a security maturity assessment model for critical infrastructure', *Procedia Computer Science*, 219, pp. 1–11.
51. ISMS.online (2025) ISO 27001:2022 Annex A explained and simplified. Available at: <https://www.isms.online/iso-27001/annex-a-2022/> (Accessed: 16 May 2025).
52. Braber, F., Hogganvik, I., Lund, M.S., Stolen, K. and Vraalsen, F. (2023) 'Model-based security analysis in seven steps: a guided tour to the CORAS method', *BT Technology Journal*, 25(1), pp. 101–117.
53. Advisera (2025) ISO 27001 risk assessment and risk treatment: the complete guide. Available at: <https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/> (Accessed: 22 April 2025).
54. Cynomi (2025) What is a cybersecurity maturity assessment? A complete guide. Available at: <https://cynomi.com/learn/cybersecurity-maturity-assessment/> (Accessed: 9 May 2025).
55. Chart.js Contributors (2023) Chart.js — simple yet flexible JavaScript charting for designers and developers, Version 4.4.0. Available at: <https://www.chartjs.org> (Accessed:

1 April 2025).

56. Duckett, J. (2021) HTML and CSS: Design and Build Websites. 2nd edn. Indianapolis: John Wiley and Sons.
57. Duckett, J. (2022) JavaScript and jQuery: Interactive Front-End Web Development. 2nd edn. Indianapolis: John Wiley and Sons.
58. Pham, H. and Park, J. (2023) 'Interactive web-based dashboards for cybersecurity situational awareness: design principles and evaluation', Computers and Security, 128, p. 103163. Available at: <https://doi.org/10.1016/j.cose.2023.103163>
59. Viking Cloud (2025) Risk-based vs compliance-based security: why one size does not fit all. Available at: <https://www.vikingcloud.com/blog/risk-based-vs-compliance-based-security-why-one-size-doesnt-fit-all> (Accessed: 30 April 2025).
60. Zero Networks (2026) Assessing cybersecurity maturity: how to benchmark your defences in 2026. Available at: <https://zeronetworks.com/blog/assessing-cybersecurity-maturity-how-to-benchmark-your-defenses-in-2026> (Accessed: 17 May 2025).
61. Wan Mohamad, W.A., Abdul Molok, N.N. and Abd Rahim, N.H. (2025) 'A conceptual framework: event-based cybersecurity risk assessment for organisations', Journal of Information Systems and Digital Technologies, 7(1), pp. 120–135. Available at: <https://journals.iium.edu.my/kict/index.php/jisdt/article/view/574> (Accessed: 3 April 2025).
62. Almohaimeed, M., Albalwy, F., Alharbi, R., Alqarni, A. and Aljohani, A. (2025) 'Developing a comprehensive cyber risk assessment framework for supply chains: insights into third-party vulnerabilities and security gaps', Intelligent Information

Management, 17(3), pp. 1–20. Available at: <https://doi.org/10.4236/iim.2025.173004> (Accessed: 10 May 2025).

63. Annunziata, G., Sheykina, A., Palomba, F., De Lucia, A., Catolino, G. and Ferrucci, F. (2024) 'Security risk assessment on cloud: a systematic mapping study', in Proceedings of the 28th International Conference on Evaluation and Assessment in Software Engineering (EASE 2024). New York: ACM. Available at: <https://doi.org/10.1145/3661167.3661287> (Accessed: 27 April 2025).
64. Siddamsetti, S., Kumar, P. and Rao, T. (2022) 'Comparative study of cyber security risk assessment frameworks', NeuroQuantology, 20(8), pp. 1–12. Available at: <https://www.neuroquantology.com> (Accessed: 6 May 2025).
65. Kutova, M. (2024) 'The framework of information security in e-governance system', Economic Synergy, 1, pp. 20–30. Available at: <https://doi.org/10.53920/ES-2024-1-2> (Accessed: 14 April 2025).
66. Hossain, M.A. and Islam, M.S. (2024) 'Trends and evolution in IT governance and system security research: a bibliometric analysis', Maliki Interdisciplinary Journal, 2(10), pp. 90–101. Available at: <https://urj.uin-malang.ac.id/index.php/mij/article/view/10118> (Accessed: 18 April 2025).
67. Da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020) 'Defining organisational information security culture — perspectives from academia and industry', Computers and Security, 92, p. 101713. Available at: <https://doi.org/10.1016/j.cose.2020.101713>
68. Georgiadou, A., Mouzakitis, S., Bounas, K. and Askounis, D. (2021) 'A cyber-security culture framework for assessing organisation readiness', Journal of Computer Information Systems, 62(3), pp. 452–462.

69. Haney, J.M. and Lutters, W. (2023) 'From compliance to impact: tracing the transformation of an organisational security awareness program', arXiv preprint, arXiv:2309.07724. Available at: <https://arxiv.org/abs/2309.07724> (Accessed: 2 May 2025).
70. International Organization for Standardization (2022) ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: ISO.
71. Ozkan, B.Y. and Spruit, M. (2021) 'Assessing cybersecurity maturity: a domain-level benchmarking approach for organisations', *Computers and Security*, 110, p. 102430.
72. Almuhaideb, A.M. and Alqahtani, M. (2022) 'Toward a comprehensive cybersecurity maturity model for Saudi organisations', *International Journal of Advanced Computer Science and Applications*, 13(4), pp. 1–10.
73. Al-Mayahi, I.H. and Mansoor, S.P. (2020) 'Information security maturity model: a framework review and analysis', in *Proceedings of the 2nd International Conference on Computer and Information Sciences*. IEEE, pp. 1–6.
74. Linkov, I., Kott, A. and Ackerman, G. (2022) 'Resilience-based cyber maturity assessment: bridging compliance and operational readiness', *Risk Analysis*, 42(8), pp. 1745–1760.
75. ENISA (2023) Good Practice Guide for Cybersecurity Maturity Assessment. Heraklion: European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu> (Accessed: 9 April 2025).
76. Johannsen, W. and Goeken, M. (2022) 'Artefact types in design science research: a structured classification model', *Business and Information Systems Engineering*, 64(2),

pp. 179–194. Available at: <https://doi.org/10.1007/s12599-021-00720-y>

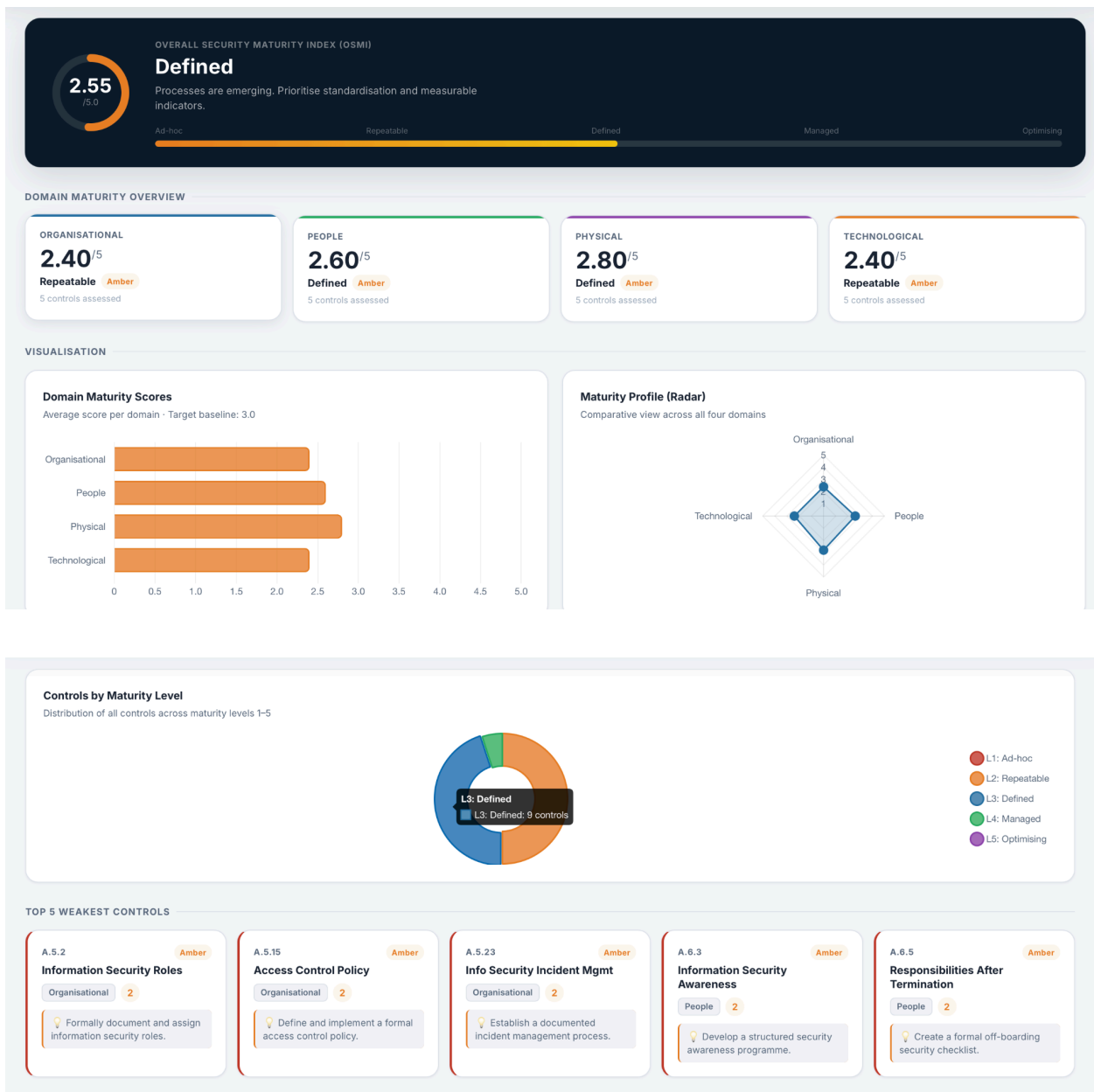
77. Iivari, J. (2021) 'A paradigmatic analysis of information systems as a design science', *Scandinavian Journal of Information Systems*, 25(2), pp. 31–77.
78. Venable, J., Pries-Heje, J. and Baskerville, R. (2021) 'FEDS: a framework for evaluation in design science research', *European Journal of Information Systems*, 30(1), pp. 1–23.
79. Myers, M.D. and Venable, J.R. (2024) 'A set of ethical principles for design science research in information systems', *Information and Management*, 61(1), p. 103903.
80. Baskerville, R., Baiyere, A., Gregor, S., Hevner, A. and Rossi, M. (2022) 'Design science research contributions: finding a balance between artifact and theory', *Journal of the Association for Information Systems*, 23(1), pp. 1–20.
81. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. and Fallon, M. (2022) *Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations*. NIST SP 800-161 Rev. 1. Gaithersburg: NIST. Available at: <https://doi.org/10.6028/NIST.SP.800-161r1> (Accessed: 7 May 2025).
82. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and McQuaid, R. (2021) *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST SP 800-160 Vol. 2 Rev. 1. Gaithersburg: NIST. Available at: <https://doi.org/10.6028/NIST.SP.800-160v2r1> (Accessed: 1 April 2025).
83. Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012, reissued 2021) *Computer Security Incident Handling Guide*. NIST SP 800-61 Rev. 2. Gaithersburg: NIST. Available at: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> (Accessed: 20 April 2025).

84. Scarlata, V., Thissen, M., Schaffer, S. and Zimmerman, T. (2023) Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. NIST SP 800-66 Rev. 2. Gaithersburg: NIST.
85. Oyeniyi, J.O. and Oyeniran, O.A. (2024) 'Optimising information security in cloud environments: a risk management approach and guide for enterprise cloud security', *Journal of Cybersecurity Education, Research and Practice*, 2024(1). Available at: <https://digitalcommons.kennesaw.edu/jcerp> (Accessed: 13 May 2025).
86. Linkov, I. and Kott, A. (eds.) (2022) *Cyber Resilience of Systems and Networks*. 2nd edn. Cham: Springer.
87. Shostack, A. (2022) *Threat Modeling: Designing for Security*. 2nd edn. Indianapolis: John Wiley and Sons.
88. ISO/IEC (2023) *ISO/IEC 27001:2022 — Information Security Management Systems: A Practical Guide for SMEs*. Geneva: ISO. Available at: <https://www.iso.org/publication/PUB100484.html> (Accessed: 18 May 2025).
89. Gambo, M.L. and Almulhem, A. (2025) 'Zero trust architecture: a systematic literature review', *Journal of Network and Systems Management*, 34, p. 25. Available at: <https://doi.org/10.1007/s10922-025-09998-x> (Accessed: 15 April 2025).
90. Ibrahim, M. and Al-Humaidan, R. (2023) 'Learning from cybersecurity incidents: a systematic review and agenda for future research', *Computers and Security*, 131, p. 103305. Available at: <https://doi.org/10.1016/j.cose.2023.103305>
91. ENISA (2022) *ENISA Threat Landscape 2022*. Heraklion: European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu> (Accessed: 30 April 2025).

92. Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L. and De Nicola, R. (2021) 'Framework, tools and good practices for cybersecurity curricula', IEEE Access, 9, pp. 94723–94747. Available at: <https://doi.org/10.1109/ACCESS.2021.3094409>
93. Chang, Y.W. and Liang, C.Y. (2023) 'Enhancing security awareness among employees in the digital transformation era: an effective behavioural training model', IEEE Access, 11, pp. 1–14. Available at: <https://doi.org/10.1109/ACCESS.2023.3299781>
94. Almohaimeed, A.A. (2024) 'Employee cybersecurity awareness training programmes customised for SME contexts to reduce human-error related security incidents', Journal of Knowledge, Learning, and Science Technology, 3(3), pp. 382–409. Available at: <https://doi.org/10.60087/jklst.vol3.n3.p382-409> (Accessed: 5 May 2025).
95. Haney, J.M., Furman, S.M. and Theofanos, M. (2021) 'Measuring and evaluating the effectiveness of security awareness programs', ISACA Journal, 5. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-5> (Accessed: 11 April 2025).
96. ISC2 (2024) Implementing ISO 27001:2022 for startups and SMEs: from theory to practice. Available at: <https://www.isc2.org/Insights/2024/03/Implementing-ISO-27001-2022-for-Startups-and-SMEs> (Accessed: 17 April 2025).
97. Niculete, A.I. and Diaconescu, A. (2022) 'Interactive security dashboards for organisational risk visibility: a design and usability study', Procedia Computer Science, 199, pp. 700–709.
98. Elrawy, M.F., Awad, A.I. and Hamed, H.F.A. (2022) 'Intrusion detection systems for IoT-based smart environments: a survey', Journal of Cloud Computing, 7(1), p. 21. Available at: <https://doi.org/10.1186/s13677-022-00218-8>

99. Whitman, M.E. and Mattord, H.J. (2021) Principles of Information Security. 7th edn. Boston: Cengage Learning.
100. Braber, F., Hogganvik, I., Lund, M.S., Stolen, K. and Vraalsen, F. (2022) 'CORAS: a structured method for risk analysis of security critical systems', International Journal of Information Security, 21(4), pp. 887–907. Available at: <https://doi.org/10.1007/s10207-022-00580-9> (Accessed: 20 May 2025).

Appendix A - DashBoard



2.55/5

Current Level: Defined

OSMI of 2.55 places the organisation at "Defined" maturity level.

Progress towards Level 5 (Optimising)

RECOMMENDED NEXT STEPS

- 1 Introduce measurement mechanisms — define KPIs and review cycles.
- 2 Conduct internal audits to verify consistent control implementation.
- 3 Integrate maturity assessments into the ISMS audit cycle.

CONTROLS ASSESSMENT DATA

Q Search controls or domain...

Reset Filter

Showing 20 of 20 controls

CONTROL ID :	CONTROL NAME :	DOMAIN :	LEVEL :	MATURITY LABEL :	RAG STATUS
A.5.1	Information Security Policies	Organisational	3 3	Defined	Amber
A.5.2	Information Security Roles	Organisational	2 2	Repeatable	Amber
A.5.9	Inventory of Assets	Organisational	3 3	Defined	Amber
A.5.15	Access Control Policy	Organisational	2 2	Repeatable	Amber
A.5.23	Info Security Incident Mgmt	Organisational	2 2	Repeatable	Amber