A Conceptual Model to Assess the Maturity Of Information Security Audit Process

Memoona J. Anwar[1], Asif Q. Gill[1] and Henderik A. Proper[2]

[1] School of Computer Science, University of Technology Sydney, Ultimo NSW, Australia
[2] Luxembourg Institute of Science and Technology, Germany

Abstract

One of the critical aspects of information security management is the security audit, both internal and external audits. The fundamental challenge for organisations is the effective design and implementation of the information security audits to better understand their information security capability. In this paper, we present insights from an action design research (ADR) project and propose a conceptual model to assess the maturity of security audit processes. The results of this research can be used to create an improvement plan, which will guide organisations to reach their target process maturity level. The maturity model proposed in this paper was evaluated by way of feedback workshops in the target organization. The model forms the basis for future work for generalising the research into a formal reference architecture (involving models and principles) for audit process maturity.

Keywords

Information Security, Information Security Audit, Process Maturity, Compliance.

1. Introduction

The goal of information security is to ensure a sustainable and adequate level of security or protection for information assets [1]. To understand security, it is critical for organisations to realise that security is a process, and not a product [2]. Therefore, it is of prime importance to assess the maturity of information security practices and procedures within an organisation. As defined by Whitman and Mattord [3], security assessment means testing a system to determine its compliance with a security model, security standard, or specific pre-defined metrics. In this context, organisations conduct information security assessment via internal and external audits against standards or regulations. Hence, the internal and external audit processes play a critical role in security assessment. Over the years, information security audits have evolved from an exercise in "box ticking" and reporting faults, to putting a much stronger emphasis on proactive risk management. However, the remaining challenge is to determine if the audit process is keeping pace with rapidly changing areas of security risks such as ransomeware, phishing attacks, cloud jacking, and deepfakes. Organisations with well-planned audit process are better able to identify security related business risks and underlying systemic weaknesses, take appropriate corrective actions, and ultimately support continuous improvement. Nevertheless, to maintain and enhance information security audit's credibility, its maturity must be measured and continually improved [4].

An information security audit process involves questioning by an internal or external party, where they seek implementation evidence for specific controls and processes. In practice, however, questions do not reveal the facts regarding their implementation. As a result, while these questions are for the betterment of all, audits frequently do not detect underlying issues. As such, they may even lead to a false sense of security. In today's digital world of ever-present cyber threats, it is unsafe for a business to approach a security audit as a tick-box exercise; the stakes are too high [5]. Instead, the audit should be used as an opportunity to build cyber resilience. Limited financial and human resources is an issue

[1]: PoEM'2022 Workshop and Models at Work Papers, November 23-25, 2022, London, UK
EMAIL: memoona.anwar@uts.edu.au (A. 1); asif.gill@uts.edu.au (A. 2); erik.proper@list.lu (A. 3)
ORCID: 0000-0001-5438-8811, (A. 1); 0000-0001-6239-6280 (A. 2); 0000-0002-7318-2496 (A. 3)

in establishment of efficient security program [6]. To ensure security, it is important to build security into the process and adapt a security architecture which ensures that regular security related tasks, are deployed correctly [7]. However, the challenge then becomes to assess the maturity of the audit process. Process maturity assurance teams have traditionally relied on manual systems, including spreadsheets and word processing applications, with reporting and communication on an infrequent or ad hoc basis due to the effort required. They are, therefore, unable to track and respond to changes within the underlying risk profile of the organisation, particularly in adapting the audit plan. This itself increases organisational risk by compromising the accuracy of audits, impacting the integrity of organisation, overlooking potentially significant risks, not informing the top management in timely manner, and not identifying the needed improvements. This research narrows the gap between theory and practice for information security management by following the process of audit maturity model and by identifying the benefits of implementing a standard for organisation's internal audit needs.

This research was conducted as part of a large action design research (ADR) project [8, 9], which was performed through the collaboration with industry partner IDZ. IDZ provides electronic identity verification services across the globe. In provision of its identity verification services, IDZ processes personal information. The security requirements for organization processing personal information are very stringent. To ensure compliance with these requirements, IDZ needs to ensure the efficiency and maturity of security processes within the organization. As part of ideation and problem formulation, IDZ highlighted that they do not have any method to assess the maturity of their information security audit processes, and we must find a comprehensive method, one that is consistent with the IDZ information security practices. Thus, the IDZ engaged University (coded name: UTX) researchers to address the following important practice-oriented research question: *RQ: How to assess the maturity of information security audit processes?*

As a first step, the project team was selected. This project team involved two researchers from UTX who actively worked (ADR intervention) with the IDZ team to design the information security audit maturity model (*i*SAM^2) artefacts for solving the problem (RQ) at hand. The core of the IDZ team members (5+) comes from business strategy (top management), project delivery (business analyst, project manager and development team) and privacy & security (internal/external auditors & information security manager) areas (see figure 1). As a result of initial research, the ADR team found that there is no set criterion based upon which the maturity of audit processes can be measured. Therefore, the initial phase aims to develop a conceptual model for *i*SAM^2 to assess the audit process maturity. The conceptual model presented in this paper provides the foundations for future development of logical and physical models for *i*SAM^2.

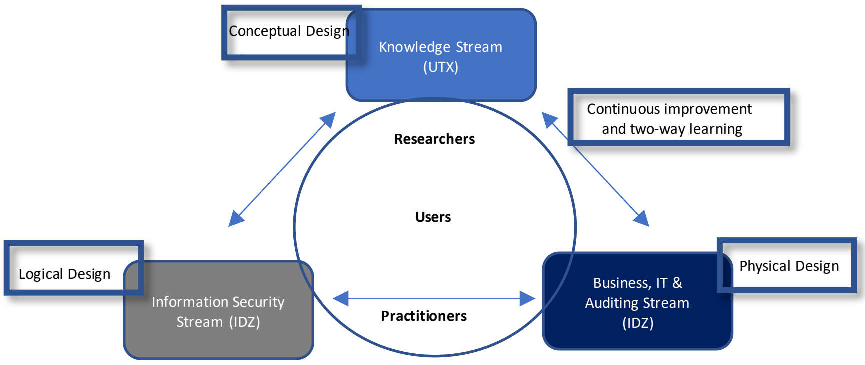
Conceptual Design
Knowledge Stream (UTX)
Continuous improvement and two-way learning
Researchers
Users
Logical Design
Information Security Stream (IDZ)
Practitioners
Business, IT & Auditing Stream (IDZ)
Physical Design

Figure 1. ADR Project Workstream

The remainder of the paper is organised as follows. We first present the literature review, based on which we identify the research gap we aim to address. Next, we discuss the research approach used in the study. We then present the *i*SAM^2 contextual and conceptual model that explains the key concepts and relationships for assessing the maturity of audit process. The evaluation of conceptual model is presented in section 6. Finally, we conclude the paper and present directions for future research.

2. Literature Review

The concept of maturity models is increasingly being applied within the field of information systems as an approach for organisational development or as means of organisational assessment [10]–[12]. In general, maturity models involve a systematic framework to benchmark an organisation's performance as well as continuous improvement processes [13]. The focus of our research is on the development of a maturity model for information security audits. There are numerous studies that have been conducted on information security [14]–[17]. Hengstler [16] and Siponen et al. [15] examine the factors related to normative beliefs, threat appraisal, self-efficacy, and visibility that influence employees' intention to comply with information security policies in organizations. Ifinedo [14] assesses the social influence of changing individual's thoughts, actions, feelings, attitudes, and behaviors on information security compliance in organisations. Kim et al. [17] investigate the factors that influence employees' information security policy compliance behaviors using elements of their "Triandis model". These studies have focused primarily on understanding employees' attitudes, and behavior on information security in organisations. There is, however, lack of research in better understanding the impact of audit process maturity on information security in organisations [18]. Information security audit process maturity is the measure of how close the audit process is to being complete and able of continual improvement through qualitative measures and feedback.

There are some model based initiatives. As an example, KPMG proposes a Cyber Maturity Assessment [19] for providing an in-depth review of organisational capability to protect information assets and preparedness against cyber-attacks. However, Cyber Maturity Assessment is focused on maturity of overall security program not just one process. Saleh [13] developed an information security maturity model which is intended as a tool to evaluate the ability of organizations to meet the objectives of security. However, it seems to lack criteria to judge the trustworthiness and relevance of the results. COBIT5 maturity model is introduced by the Information Systems Audit and Control Association [20]. Information Security Management Maturity Model [21] is used to evaluate the level of security maturity in an enterprise information system, improve information systems by gap analyzing and prioritizing the investment process. The Publisher's Program Overview for Information Security Management Assistance, known as PRISMA, was presented in 2007 by the NIST7358 [22]. The Information Security Maturity Model is another popular maturity model introduced by Woodhouse in 2008 [23]. Another security framework has been introduced by IBM called ISF [24]. The Cyber-security Capability Maturity Model (C2M2) was presented in 2014 [25]. The model introduces five different dimensions. A maturity model derived from ISO 27K [26], [27] is introduced by Brotby and Hinson [28], which covers the 12 domains of this standard. The focus of above mentioned models is one of the following: risk management [25]–[28], security policy and plan management [26]–[28], human resource management [21], [23], [25]–[28], physical security management [21], [26]–[28], IT security management [26]–[28], communication security management [25], security technology management [21], [26]–[28], security event and incident management [21], [22], [25]–[28] or security audit and compliance management [21], [22], [25]–[28]. To the best of our knowledge there is no model that focuses on maturity of audit process. The iSAM2 takes a holistic approach to cover all aspects of information security audit.

3. Research Gap

None of the above reviewed studies focuses on assessing the maturity of information security *audit processes*. Hence, there is a need to develop such a model that can help organisations in implementing the fundamentals of effective internal auditing regardless of industry or sector.

Assessing the maturity of audit process will help organisations obtain a better view of, and understand the deviations from, the audit process workflow. This in turn will highlight the information security risks that organisation might be facing, and how these can be remediated. The main objective of such maturity model is to identify a baseline to start improving the audit process for quality improvement, cost reduction and delivery-time reduction. The maturity model then is used in cycles to build consensus, set the priorities of investment in information security, and finally measure the implementation progress [29]. Some of the frameworks that we studied come with maturity model such as COBIT and ISF. Some other frameworks do not have maturity model such as ISO 27001. Hence, in this paper we build the foundations of *i*SAM^2 based on ISO 27001. The reason for selecting ISO 27001 is because it is an international standard, independent of any specific industry. Furthermore, IDZ is already ISO 27001 compliant and wanted to validate the model for ISO 27001 as a starting point. However, the approach proposed in this paper can be adapted to other standards, which is subject to further research.

Theoretically, this study contributes to the information systems research by better understanding the measures of maturity of audit process and how they can be used as a baseline for enhancing information security in organisations. Practically this study informs information security auditors and policy makers on the major institutional drivers for influencing information security in organisations. In addition to implementation challenges, accomplishing best practices in the audit process is needed and it was undertaken in this research in the form of a self-study that organisations would use to measure effectiveness and efficiency of audit process.

4. Research Approach

This research project applied the ADR [8], [9] method for solving the practical design problem of designing a maturity assessment model for a well-run information security audit. The starting point for this research was IDZ's interest in developing a comprehensive yet straightforward and adaptive framework to address the above research question. We answered this vital practice-oriented research problem by using the ADR method [8, 9]. This ADR project developed an overall blueprint of the broad adaptive digital identity reference architecture framework, which is organized into three main components: assess, design, and evolve [30]–[34]. Before designing the overall reference architecture as a privacy enabler for identity verification process, IDZ wanted to know how mature their internal audit process is to identify security risks and gaps accurately. Hence, this project commenced in November 2018 at the IDZ, Sydney, Australia, and continued until Dec 2020. Researchers from UTX were approached by the IDZ in 2018 to help in designing a secure digital identity verification framework. This *i*SAM^2 is part of that broad framework for assessing the effectiveness and efficiency of information security internal audit process.

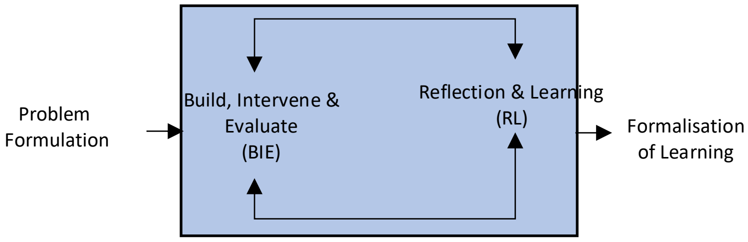
Problem Formulation
Build, Intervene & Evaluate (BIE)
Reflection & Learning (RL)
Formalisation of Learning

Figure 2. Action Design Research Stages

The ADR method is formalized into four stages: problem formulation, build, intervene and evaluate, reflection and learning, and formalization of learning. The project research problem was initiated by the IDZ as a strategic initiative (practice driven). In the initiative stage, research problem for the project was discussed during the research idea workshops and meetings with the IDZ. The idea of developing the *i*SAM^2 was mutually explored by the IDZ and UTX. The IDZ had the known practical problem in hand but no known solution. One of the IDZ's internal review reports highlighted that "*there is no off-the-shelf mean to measure the effectiveness and efficiency of internal audit process*". Therefore, the challenge is the design and implementation of the *i*SAM^2. Thus, the next step is the proposed *i*SAM^2, its iterative development and evaluation. In ADR, kernel theories (See Table 1) are used to provide baseline generic elements for designing context-specific ADR artefacts. The kernel theories used in this research are adaptive enterprise service system (AESS) [35], design thinking [36], ISO 27001 [1] and a model-driven architecture approach [37]. The ADR team combining researchers and industry professionals applied the AESS framework as a meta-framework in this research project. The AESS was used because it provides a vendor-independent, layer-based digital ecosystem metamodel, which was used to inform the development of the *i*SAM^2 for end-to-end digital ecosystem [30]. Figure 2 shows the approach adopted for this research.

Table1
Kernel Theories

#	Item	Description
1	ISO 27001-2013	Although *iSAM^2* is not standard specific however IDZ's client requirement is that they should be ISO 27001 certified. Therefore, we used ISO 27001 as a starting point.
2	Adaptive enterprise service system (AESS)	To design the *iSAM^2*, we needed the reference meta-model. Thus, we used the AESS, which provided an end-to-end digital ecosystem view to design the *iSAM^2*. The purpose of the *iSAM^2* was to design a reference maturity model with different maturity levels considering security of humans, technology, facility, and environment. This has been further explained in detail in the paper (e.g., see Fig. 3).
3	Design thinking (DT)	Design thinking offers a balanced approach or mindset of intuition and analytical thinking, which was used for the continuous design or re-design of the *iSAM^2* in small iterations based on the feedback loop mechanism. Design thinking is clear in the four stages of applied ADR.
4	Model Driven Architecture	Model-driven architecture provides a set of guidelines for the structuring of specifications, which are expressed as models. The *iSAM^2* was organised and explained in terms of these layers.

5. Information Security Audit Maturity Model-Conceptual Model

The ADR team (See Figure 1) at the IDZ engaged in recursive adaptive cycles of design innovation and mutual learnings among the project work streams at conceptual, logical, and physical architecture design layers (Model Driven Architecture layers based on architecture kernel theory). The scope of this research paper is limited to conceptual model only. The researchers from UTX largely contributed to the conceptual design and mutual learnings through their knowledge of design theory and technological advances (knowledge stream – Figure 1), while the IDZ practitioners including supporting organisations largely contributed through their practical knowledge of IDZ work practices and the environment in which the IDZ operates (integration of research and practice). Users were involved in all aspects of this process. The knowledge stream (researchers) was mainly responsible for the conceptual *i*SAM^2 architecture model. The information security stream (practitioners) was responsible for turning the conceptual architecture into the logical *i*SAM^2 model, and the business, IT and auditing stream (practitioners) was responsible for turning the logical *i*SAM^2 into the physical *i*SAM^2 or implementation (planning, fieldwork and reporting). These three streams also include users. The next section presents the contextual and conceptual model for *iSAM^2*.

5.1. Contextual Model (Level-0)

Figure 3 illustrates the *iSAM^2* architecture context model (level 0) for the IDZ, which highlights the four major architecture building blocks of the IDZ: audit, compliance, information security framework and asset. This model shows that security compliance is based on information security framework and is assured by security audit (both internal & external). Information security framework is developed and maintained to make organisational assets (identity information in IDZ's context) secure. Hence, it is very important to have an efficient and effective audit process in place to measure organisation's security preparedness correctly. These four building blocks were detailed in terms of conceptual (level 1), logical (level 2) and physical models (level 3). In this paper, we present the details of contextual and conceptual models as examples.

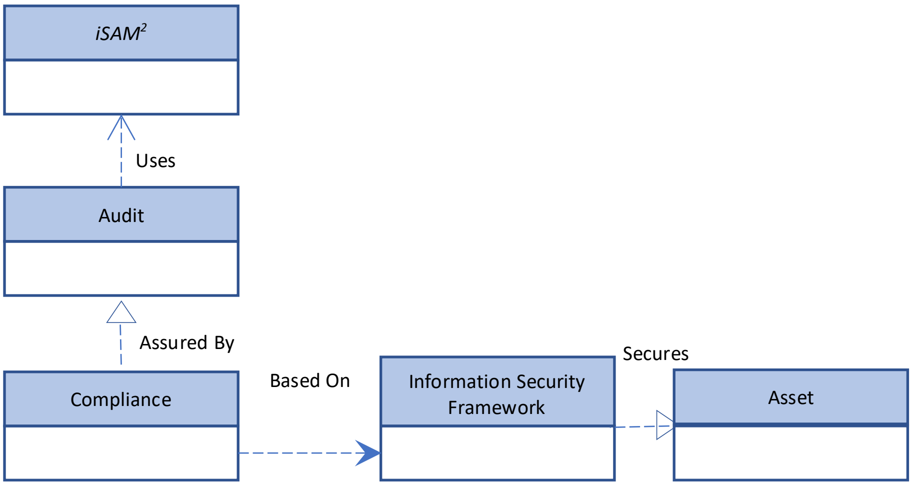

Figure 3. *i*SAM² Context Model (Level 0)

5.2. Conceptual Model (Level-1)

The *iSAM²* model is based on the theoretical AESS metamodel. In practice, an architecture is designed using some relevant reference or metamodel; thus, in this project, we used the vendor independent AESS metamodel as a reference model to develop the *iSAM²* architecture for the IDZ context.
This metamodel was used due to its higher relevance to IDZ's identity ecosystem. The identity ecosystem is a user-centric (HUMAN) online environment (ENVIRONMENT) – a set of processes, technologies (TECHNOLOGY), policies and agreed upon standards that securely (PRIVACY &

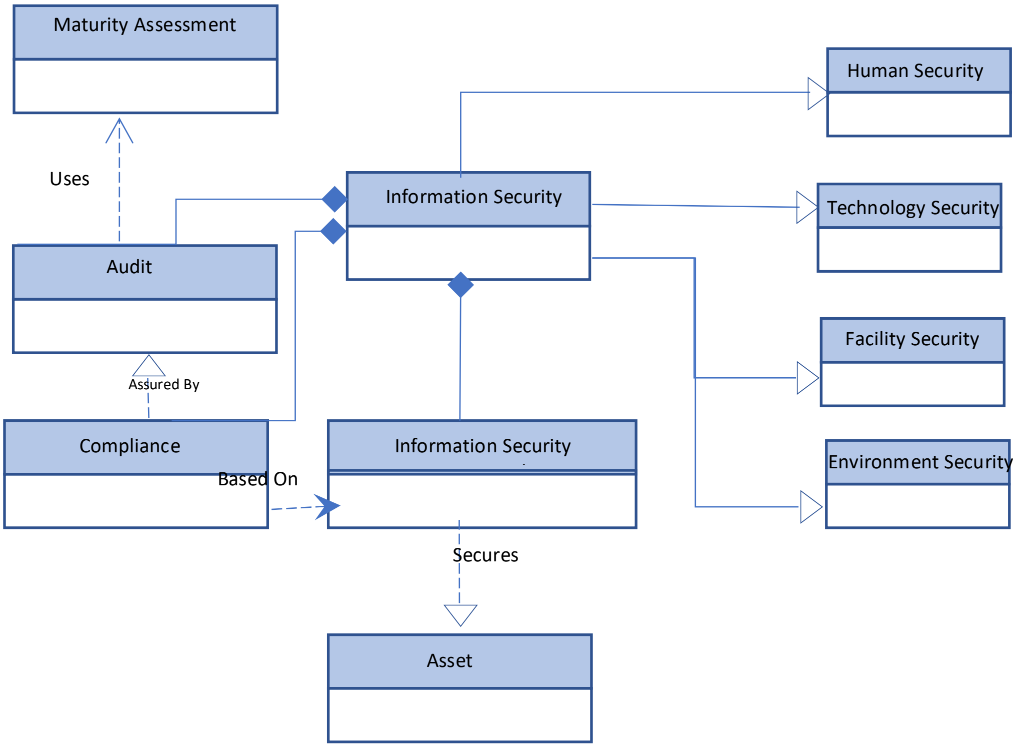

Figure 4. *i*SAM² Conceptual Model (Level 1: Security Classification) (Based on AESS)

SECURITY) supports transactions ranging from anonymous to fully-authenticated and from low to high value based upon data stored in secure data centers (FACILITY) [38], [39]. This section discusses the *i*SAM^2 conceptual architecture models for information security audit maturity.

Audit and compliance are both very essential functions in an organisation. Audit and compliance have risen in importance, both signifying critical control components of information security. The compliance function is meant to reasonably ensure that the company is complying with all applicable laws, rules, and regulations, as well as internal codes of conduct, policies and procedures managed via company's information security framework. The audit function is designed to monitor and evaluate the company's internal control environment as to its adequacy, efficiency, and effectiveness. There are two types of conceptual security models at level 1: security classification model (See Figure 4) and security concepts & relationship model (See Figure 5). The information security building block is core to the security architecture and was classified in terms of human, technology, facility, and environment security. The security concepts and relationship conceptual model described the relationship between these layers. There is a two-way relationship between human security, technology security and facility security. The human, technology and facility security are dependent on environment security in which they operate. The security of environment in turn is governed by multiple factors such as changing risk, information security needs, external context, control objectives policies, laws, regulations, and compliance requirements.

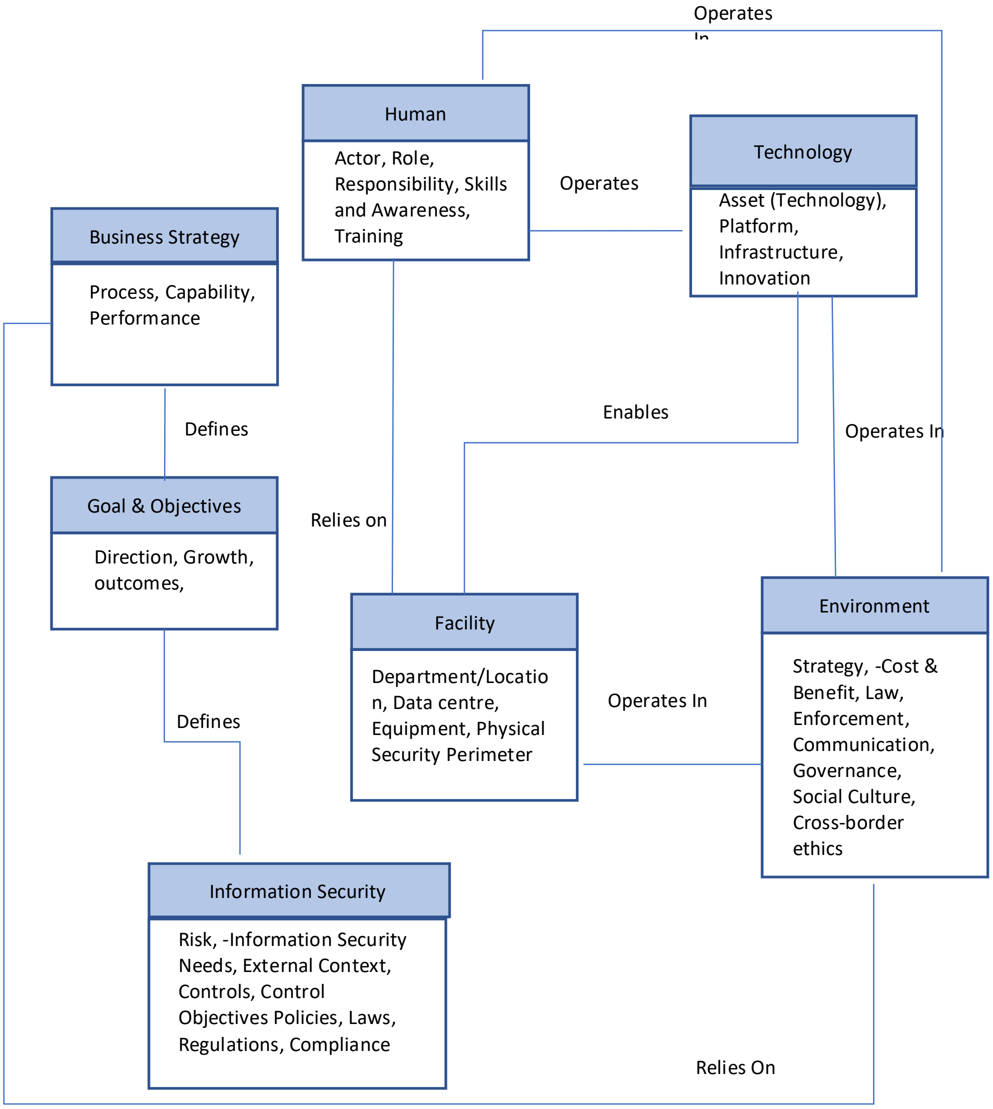
Operates In
Human
Actor, Role, Responsibility, Skills and Awareness, Training
Operates
Technology
Asset (Technology), Platform, Infrastructure, Innovation
Business Strategy
Process, Capability, Performance
Defines
Enables
Operates In
Goal & Objectives
Direction, Growth, outcomes,
Relies on
Facility
Department/Location, Data centre, Equipment, Physical Security Perimeter
Operates In
Environment
Strategy, -Cost & Benefit, Law, Enforcement, Communication, Governance, Social Culture, Cross-border ethics
Defines
Information Security
Risk, -Information Security Needs, External Context, Controls, Control Objectives Policies, Laws, Regulations, Compliance
Relies On

Figure 5. *i*SAM^2 Conceptual Model (Level 1: Concepts & Relationships) (Based on AESS)

6. iSAM^2 Evaluation

The *i*SAM^2 model progressed through the contextual (Level-0) to physical model (level-3). Despite its traditional linear design and post-design evaluation, *i*SAM^2 was iteratively built and evaluated. The primary purpose of building and evaluating *i*SAM^2 in iterations was to enable progressive emergence of the design (from contextual to the physical model) as each component is progressed through build, intervene, and evaluate and reflection and learning iterations. Hence, the next step is to demonstrate the indictive evaluation of *i*SAM^2.

Following the definition proposed by Wynekoop and Russo [40], evaluation of a conceptual model is described as the analysis of the conceptual model to verify its usefulness, effect or impact. For the evaluation of conceptual model, we demonstrate the completeness, usefulness, and generalization (See Table 2) of our model as the conceptual foundation to design a broader adaptive digital identity reference architecture framework. In this paper, we used feedback driven approach by conducting workshops with all stakeholders.

Table 2

Evaluation Criteria

Metric	**Description**
Completeness	The number of concepts present in the model corresponds to the number of concepts demanded by the user in their requirements.
Usefulness	*i*SAM^2 is useful for filling the research gaps
Generalization	*i*SAM^2 is general and is not attached to one context or situation. Furthermore, it can adapt to multiple circumstances and be applied with different technology stacks.

During the workshop, the researchers presented the research problem and gaps identified by the literature review. The presentation ran for 30 minutes. After the presentation, the researcher facilitated a brainstorming session to identify the alignment between IDZ's needs and the research problem for this research project. Table 3 details the first design workshop together with the workshop objectives, role and responsibilities and feedback and comments from the participants.

At the end of the design workshop all participants agreed that the concepts and relationships in the *i*SAM^2 conceptual model fulfill the criteria of completeness, usefulness, and generalization. The overall goal of this research was to develop and test design principles and practices to address the identified research problem assessing the effectiveness and efficiency of the internal audit via maturity model design and implementation. This paper only presents the details of first iteration of *i*SAM^2 development, however as a result of feedback workshop two important design principals were emerged i.e., critical asset identification and setting out clear information security objectives. The design principals will be further evaluated on formalizing the learning and final feedback at the end of the project. The ADR team is ready to start the next iteration of build, intervene, and evaluate and reflection and learning. the results of further iteration will be presented as future work.

Table 3

iSAM2 Conceptual Model Design and Review Workshop

Organization:	IDZ (coded name) is a leader in the eIDV (Electronic Identity Verification) industry with the capability to provide access to the widest, most in-depth, reliable, and independently sourced identity data throughout the APAC region.	
Workshop Objective	To evaluate iSAM2 Conceptual Model	
Workshop Facilitator	The researcher of this project is responsible for explaining the model concepts and relationships, educating, and facilitating the design decisions, and documenting the feedback	
Workshop Participants	• top management • business analyst • project manager • development team • internal/external auditors • information security manager	
Main Design/Evaluation Component	*i*SAM^2 Conceptual Model	
Role/Responsibility	**Comment/Suggestion/Feedback**	**Criteria**
Top Management	*"The existing audit procedure for IDZ, whilst efficient and seamless, must be improved in order to maintain and extend compliance status within the industry."*	Usefulness Applicability
Development Team	*"IDZ is seeking to harness the potential of new global technology trends involving biometrics and blockchain. Incorporating these technologies into enhanced applications and efficient operations that its' clients can leverage will open doors for implementation of new global standards. The model covers the foundational concepts of mostly standards."*	Generalization
Auditors	*"With changing technological and regulatory landscapes, the audit and compliance requirements will change, the models covers all aspects of technology as well as environmental changes including legal. Which implies its adaptability."*	Usefulness Generalization completeness

7. Conclusion and Future Work

In this research, we address a practice-oriented research problem by applying the ADR method for assessing the maturity of information security audit process using Information Security Audit Maturity Model (*i*SAM^2). The scope of this paper is limited to the contextual and conceptual model of *iSAM^2*. The *i*SAM^2 is a novel concept in the area of process maturity assessment. The *i*SAM^2 will help in identifying key concepts and their relationships to be considered when assessing the maturity of the audit process. In order to assess the maturity of audit process, organisations can proactively identify the risks associated with the key concepts and escalate through defined path to the stakeholders in coordination with external and internal auditors. This is research in progress paper, which sets the foundation for further evaluation and formalization of the results into a reference model and principles for audit maturity, which is currently a gap both in literature and practice. The results of this paper conclude that for an audit process to be mature, it must be complete in its usefulness, reliable in information and continuously improving. The conceptual model as presented in this paper was developed during first iteration of ADR's BIE (Build, Iterate, Evaluate) cycle (See Figure 2). Further iterations of BIE in this project will be reported in future research communications.

8. References

[1] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *J. Inf. Secur.*, vol. 4, pp. 92–100, 2013, doi: 10.4236/jis.2013.42011.

[2] C. Jackson, *Network security auditing*. Cisco Press, 2010.

[3] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. 2011.

[4] F. Doig, "The all-important link between audit maturity and risk management," 2019. https://www.ideagen.com/thought-leadership/blog/the-all-important-link-between-audit-maturity-and-risk-management (accessed Nov. 17, 2021).

[5] M. Vunk, N. Mayer, and R. Matulevičius, "A framework for assessing organisational it governance, risk and compliance," in *Communications in Computer and Information Science*, 2017, vol. 770, pp. 337–350, doi: 10.1007/978-3-319-67383-7_25.

[6] N. Mayer, "A cluster approach to security improvement according to ISO/IEC 27001," 2010.

[7] S. H. Amer and J. A. Hamilton, "Understanding security architecture," in *Proceedings of the 2008 Spring Simulation Multiconference, SpringSim'08*, 2008, pp. 335–342, doi: 10.1145/1400549.1400596.

[8] A. Q. Gill and E. Chew, "Configuration information system architecture: Insights from applied action design research," *Inf. Manag.*, vol. 56, no. 4, pp. 507–525, 2019, doi: 10.1016/j.im.2018.09.011.

[9] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, "Action design research," *MIS Q. Manag. Inf. Syst.*, vol. 35, no. 1, pp. 37–56, 2011, doi: 10.2307/23043488.

[10] Ahern Dennis, C. Aaron, and T. Richard, *CMMI® Distilled: A Practical Introduction to Integrated Process Improvement, Third Edition*, vol. 39. 2008.

[11] T. Mettler and P. Rohner, "Situational maturity models as instrumental artifacts for organizational design," *Proc. 4th Int. Conf. Des. Sci. Res. Inf. Syst. Technol. DESRIST '09*, 2009, doi: 10.1145/1555619.1555649.

[12] M. B. Chrissis, M. Konrad, and S. Shrum, *CMMI - Guidelines for process integration and product development*. 2003.

[13] M. F. Saleh, "Information Security Maturity Model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 3, p. 21, 2011, Accessed: Nov. 17, 2021. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.221.1617&rep=rep1&type=pdf#page=26.

[14] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects

of socialisation, influence, and cognition," *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, 2014, doi: 10.1016/j.im.2013.10.001.

[15] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation," *Computer (Long. Beach. Calif).*, vol. 43, no. 2, pp. 64–71, 2010, doi: 10.1109/MC.2010.35.

[16] S. Hengstler, "Culture matters - A cross cultural examination of information security behavior theories," in *16th International Conference on Wirtschaftsinformatik*, 2021, vol. 2966, pp. 57–71.

[17] D.-J. Kim, I.-H. Hwang, and J.-S. Kim, "A Study on Employee's Compliance Behavior towards Information Security Policy : A Modified Triandis Model," *J. Digit. Converg.*, vol. 14, no. 4, pp. 209–220, 2016, doi: 10.14400/jdc.2016.14.4.209.

[18] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, 2012, doi: 10.1016/j.im.2012.04.002.

[19] KPMG, "The role of internal audit in cyber security readiness," 2019.

[20] ISACA, "A Business Framework for the Governance and Management of Enterprise IT." 2012, Accessed: Nov. 17, 2021. [Online]. Available: http://linkd.in/ISACAOfficial.

[21] The Open Group, *Open Information Security Management Maturity Model (O-ISM3), Version 2.0*. 2017.

[22] PRISMA, "Program Review for Information Security Assistance | CSRC," 2016. https://csrc.nist.rip/library/NIST IR 7358.pdf (accessed Nov. 17, 2021).

[23] S. Woodhouse, "An ISMS (im)-maturity capability model," in *Proceedings - 8th IEEE International Conference on Computer and Information Technology Workshops, CIT Workshops 2008*, 2008, pp. 242–247, doi: 10.1109/CIT.2008.Workshops.46.

[24] A. Buecker, M. Borrett, C. Lorenz, and C. Powers, "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security," pp. 1–80, 2010, Accessed: Nov. 17, 2021. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=K3bJAgAAQBAJ&oi=fnd&pg=PP1&dq=Using+the+IBM+Security+Framework+and+IBM+Security+Blueprint+to+Realize+Business-Driven+Security,+in+ibm',+2013.&ots=70p6pzKxb2&sig=pSMbhHbwsnnIXvbPmn6bwcOxFEk.

[25] U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2) | Department of Energy," 2014. Accessed: Nov. 17, 2021. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[26] N. Halvorson, "Information Risk Management," in *Information Security Management Handbook, Sixth Edition, Volume 2*, 2008, pp. 71–81.

[27] ISO27002Security, "ISO/IEC 27002 code of practice," *ISO27002Security*, 2017. https://www.iso27001security.com/html/27002.html (accessed Nov. 17, 2021).

[28] W. K. Brotby and G. Hinson, "- Why Measure Information Security?," in *PRAGMATIC Security Metrics*, 2013, pp. 32–47.

[29] KPMG, "Transforming Internal Audit: A Maturity Model from Data Analytics to Continuous Assurance," 2015.

[30] M. J. Anwar and A. Q. Gill, "A review of the seven modelling approaches for digital ecosystem architecture," in *Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019*, Jul. 2019, vol. 1, pp. 94–103, doi: 10.1109/CBI.2019.00018.

[31] M. Anwar, A. Gill, and G. Beydoun, "A review of Australian information privacy laws and standards for secure digital ecosystems," *ACIS 2018 Proc.*, Jan. 2018, Accessed: Oct. 10, 2022. [Online]. Available: https://aisel.aisnet.org/acis2018/36.

[32] M. Anwar, A. Gill, and G. Beydoun, "Using Adaptive Enterprise Architecture Framework for Defining the Adaptable Identity Ecosystem Architecture," *ACIS 2019 Proc.*, Jan. 2019,

Accessed: Oct. 10, 2022. [Online]. Available: https://aisel.aisnet.org/acis2019/94.

[33] M. J. Anwar, A. Q. Gill, F. K. Hussain, and M. Imran, “Secure big data ecosystem architecture: challenges and solutions,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2021, no. 1, pp. 1–30, Dec. 2021, doi: 10.1186/S13638-021-01996-2/TABLES/13.

[34] M. J. Anwar, A. Q. Gill, D. Farookh, H. Dr, and G. Beydoun, “Adaptive Digital Identity Verification Reference Architecture (ADIVRA) Framework,” Sydney, 2021. Accessed: Jul. 25, 2022. [Online]. Available: http://hdl.handle.net/10453/153306.

[35] A. Q. Gill, *Adaptive Cloud Enterprise Architecture*, vol. 4. 2015.

[36] M. Mandviwalla, “Generating and justifying design theory,” *J. Assoc. Inf. Syst.*, vol. 16, no. 5, pp. 314–344, 2015, doi: 10.17705/1jais.00397.

[37] OMG.Org, “Model Driven Architecture (MDA) | Object Management Group,” *Https://Www.Omg.Org/Mda/*, 2019. https://www.omg.org/mda/ (accessed Nov. 17, 2021).

[38] United States Government, “National Strategy for Trusted Identities in Cyberspace,” *Online*, p. 25, 2011, Accessed: Nov. 17, 2021. [Online]. Available: https://archive.epic.org/privacy/nstic.html.

[39] A. Q. Gill, “Applying agility and living service systems thinking to enterprise architecture,” in *Decision Management: Concepts, Methodologies, Tools, and Applications*, vol. 1–4, 2017, pp. 487–502.

[40] J. L. Wynekoop and N. L. Russo, “Studying system development methodologies: an examination of research methods,” *Inf. Syst. J.*, vol. 7, no. 1, pp. 47–65, Jan. 1997, doi: 10.1046/J.1365-2575.1997.00004.X.