International Journal of Innovative Computing 8(2) 23-32

UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Development of Metamodel on Information Security Risk Audit and Assessment for IT Assets in Commercial Bank

Clement Chen Kai Wen, Siti Hajar Othman, Maheyzah Md Sirat
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
kaiwen72@ymail.com, hajar@utm.my, maheyzah@utm.my

Submitted: 9/01/2018. Revised edition: 16/05/2018. Accepted: 21/05/2018. Published online: 31/05/2018

***Abstract*—Nowadays, most fortunes of the commercial banks today are linked with Information Technology (IT) assets they possess and the way they audit their organizations IT assets. As information assets become the heart of commercial banks, Information Security Risk Audit and Assessment (ISRAA) is increasingly involved in managing commercial banks information security risk situations. ISRAA is an activity that analysis, audit, mitigates, and monitors the risks associated with IT assets. A more comprehensive and tighter regulatory environment is expected through the improvement on the ISRAA with clearer and appropriately defines regulatory guideline. This research creates a unified view of ISRAA in the form of a metamodel that can be seen as a language for this domain. A metamodeling process is applied to ensure that the outcome metamodel is complete and consistent. The metamodel is validated and refined to serve as a representational layer to unify, facilitate and expedite access to ISRAA expertise.**

***Keywords*—ISRAA, Metamodel, IT Asset, Commercial Bank**

I. INTRODUCTION

In early 20th century, most of the commercial banks primary security focus is to protect their physical assets. But in modern banking, information assets become critical and linked to banks survival. Banks needed to adopt advancement of technologies from early days to match customer expectations while provides efficient service standards at all times to stay competitive among other.

As information assets become the heart of commercial banks, information security risk audit and assessment (ISRAA) is increasingly involved in managing commercial banks information security risk situations. ISRAA is an activity that analysis, audit, mitigates, and monitors the risks associated with information assets. It is expected that a more comprehensive model and tighter regulatory environment through the improvement of the risk audit and assessment because the regulatory guidelines are clearer and more appropriately describe [1].

II. PROBLEM AND CHALLENGES IN ISRAA MODEL FOR IT ASSET IN COMMERCIAL BANK

In the field of information security, lots of ISRAA models have been developed to help organizations to audit, assess, mitigate, and control their information assets to minimize information security risks. Unfortunately, most of the ISRAA models are macro type of models which are limited to certain domain and it usually applied standard process that are widely used in commercial banks today. Therefore, recent research paper suggested that research activities need to priorities on improving the limited static and scope of risk analysis to build a comprehensive information security ISRAA model on commercial banks [2].

Denial of service, sniffing, spoofing, SQL injection, and other information security issues that can compromise the security requirement confidentiality, integrity, and availability (CIA) can be found anywhere around the organization today

and not limited to commercial banks only. In order to solve the problem, a structured ISRAA model is important to ensure that information assets of banks are protected and secure from vulnerable. Therefore, commercial banks can use effective ISRAA metamodel to identify the efficient ways to audit, assess, mitigation, and control the information assets from threat and risk [3].

Knowledge on information security risk audit and assessment is still sparse and lacking in terms of availability of comprehensive ISRAA metamodel metrics that can diagnose risk exposure levels of banking organizations more effectively. Thus, it can be construed that the current state of ISRAA model is inadequate and in need of enhancement for better ISRAA to protecting their data from risk either from natural disasters or malicious activity [4].

The importance of information to modern banking sector cannot be ignored. Therefore, the risk management, governance, compliance, audit, and assessment issues within information security have become the core of organizational strategy planning. Investment and research in ISRAA fields also grew steadily in 2008 to USD 3.2 billion, an increase of 7.4% from 2007 [5].

Existing cybercriminal on commercial banks are becoming one of the highest criminal rates activities todays. Risk that threating commercial banks information assets are rapidly increasing and can be found on most of the commercial banks today from natural disaster to malicious activity. ISRAA metamodel is a critical component for commercial banks to protect and strengthen their information security level [6]. An efficient ISRAA metamodel can enhance commercial banks management to identify the best approach to audit their information assets. The current ISRAA models often lack specific guidance on how to proactively to audit commercial banks risks. Therefore, most of the financial institutions face significant risk internally and externally to commercial banks information assets especially in Southeast Asia countries like Malaysia, Singapore, Thailand and other. For example, 401k enterprise third party will have access to confidential employee data. Another example is an offshore development organization can access to critical server resources and network connection to commercial banks infrastructure. These areas have not been properly audited and assessed in the commercial banks risk profile [5].

Thus, the research objectives here are:

i. To study and identify all the important concepts used in the Information Security Risk Audit and Assessment processes
ii. To unify the Information Security Risk Audit concepts into the Information Security Risk Audit and Assessment metamodel by using a metamodelling approach
iii. To validate the proposed Information Security Risk Audit and Assessment metamodel by using metamodel validation techniques: (i) comparison against other model and (ii) face validation

And the scope of the research covered:

i. The research requires highly collaboration from related university, people, and from both domestic and foreign commercial banks. The research leveraged University Technology Malaysia huge research contribution in term of resource, facility, data, paper, journal, and ideas from all the relevant faculty and departments until the end of the research.
ii. Most of the information and data used for this research contributed from previously similar IRSA model research that done on similar or different domain and areas. Expert from information security domain will contribute in term of ideas sharing to develop new ideas on the research topic.
iii. Commercial banks e.g. DBS Bank from Singapore, Public Bank from Malaysia, and UOB Bank from Singapore will be the case study for this research paper and the methods of validation would be using qualitative assessment medamodel validation techniques which are comparison against other model and face validation with managerial level or IT staff will be selected from these bank.

The aim of the research is to Identify and propose an effective and comprehensive Information Security Risk Audit and Assessment (ISRAA) metamodel that can be used in current world based on previous research result and IT security expert ideas to developed new ISRAA metamodel to be implements on commercial banks and the metamodel being validate using comparison against other models, face validation, expert review from UTM computing department staff and collaboration from commercial banks profession.

III. LITERATURE REVIEW

This section will analyse and explain the domain of the research related literature review. It enable researcher and readers to understand the literature of research from existing research paper related to this Information Security Risk Audit and Assessment on Information Technology asset of commercial bank domain. Metamodeling, Metamodel framework, Metamodeling process, Metamodel benefits, Metamodel development, and Metamodel validation techniques related studies also provided and explained in this section.

A. IT Information Assets

On the way to apprehend information and the way to audit, defend, and manage. Information asset is a frame of information that managed and defined as a single unit so it could be assess, protect, exploited, shared, and understood correctly. It is critical to first comprehend what it means through the term information asset and how this description can streamline the process. Information assets have recognisable and plausible content material, value, lifecycles, and risk [7].

Some enterprise may additionally already have assets they can use to assist on this process. As an instance, technical surroundings registers, documentation of previous statistics audits, configuration control databases or software asset lists. Alternatively, business might have job role similar to Information Asset Proprietors, a position which become recognized via the data handling evaluate and mandated through the cabinet office (Vilcahuamán *et al.*, 2017). One should explore these resources and adapt them anywhere possible. However, they may be simplest completely primary foundation to begin with. But, it is almost genuinely be additional information business may need to acquire to identify information assets. This is simplest to begin with complex and massive definitions after then splitting the information to a reasonable grouping till appropriate size. To determine whether or not something is an information asset, it can be identified by answering the following questions:

TABLE I. QUESTION THAT DEFINE INFORMATION ASSET[9]

Value	Would it have an effect on operational efficiency if you could not access the information easily? Does it have a value to the organisation? Will it cost money to get this information again?
Risks	A risk arising from inappropriate disclosure? Is there a risk of losing the information? A risk that someone may try to tamper with it? A risk that the information is not accurate? Is there a risk associated with the information?
Content	Does it include all context associated with the information? Do you understand what it is and what it is for? Does the group of information have a specific content?
How to manage it	Will they be disposed of in the same way and according to the same rules? Were all the components created for a common purpose? Does the information have a manageable lifecycle?

B. Information Assets in Commercial Bank

In commercial bank, system is consider one of the information assets to commercial banks as all information of banks client will be store in information systems and services that process, store or transmit protectively and securely marked information. For example, in Malaysia we have CCRIS which stand for Central Credit Reference Information System is a system created by National Bank of Malaysia (Bank Negara Malaysia in Malay) to synthesis credit information regarding potential borrowers or a borrower into standardised credit reports. The system is critical as it contain important information of clients such as client credit histories. Besides CCRIS, there are also variant type of system commercial banks used such as local payment system, customer account management system, allowance payment system, and more [10].

Applications software that are used by commercial bank for managing, controlling, updating, and providing the e-banking services process. There is plenty of application software used by commercial banks to provide e-banking services such as mobile application platform (CimbClicks, Maybank2U) developed applications, operative systems, and firmware devices [11].

Some of the physical or hardware components of information assets for commercial bank consist of commercial bank hardware which is physical equipment necessary to perform banking services such as computer, printers, mobile, servers, or hand-held devices etc. Secondly, commercial bank requires networking services in order to communicate, transferring, store, and manage information for their client. Thus, networks devices such as routers, switches, hubs, cables, gateways, intrusion prevention system, and other networking related devices are considers as information assets for commercial bank. Next, commercial bank facilities included as information assets as it is the heart and physical location that providing the physical banking services. Some example of commercial bank facilities included offices, buildings, shop-lot, branch, and vehicles [9].

Information assets also included personal data or information of client on commercial bank. By personal information or data that any data linking to an identifiable individual or individuals with data about them whose if disclose would put them in a significant risk, distress, and danger situation. This includes data approximately any person whether or not it is a claimant, member of team of workers or a contractor. For example, information containing a claimant or individual name, identification card number, insurance number, phone number, driving licence details, home address, bank details, databases, and documentation such as user manuals, contracts, standards, etc [9].

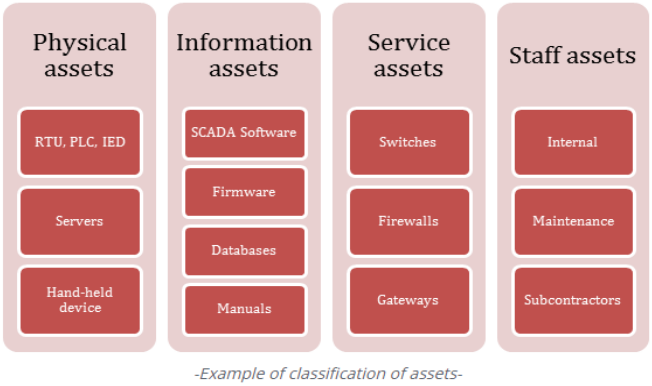

Fig. 1. Example of Classification of Asset [9]

Staff also treated as assets in commercial bank such as staff from the organisation as well as subcontracted staff, maintenance staff and in general, all those that have access in one way or another to the banks [9]. Managing of information assets can be convenient by classify variant type of assets into categories according to their domain and specification:

C. Commercial Bank

A commercial bank is sort of financial organization that accepts deposits, offers bank account services, provide commercial, non-public, mortgage, hire purchase, and personal loans. Basic financial products services like fixed deposit and savings accounts for individuals, business, and agencies. A financial institution (bank) is where most of the people do their banking, rather than an investment financial institution [12].

Due to the development and rely of information technology in commercial banks from wide areas of services such as online transferring, database, server, networking, and software application for e-banking services. Information security becomes increasingly more valuable to commercial banks. Strategies to provide the robust protection of data and information security and handy e-banking software application environment has turned out to be major focus of commercial banks. In United States with the high level of dependence of technology, the financial annual losses are approximately 75 billion dollars due to e-banking services related type of security threat and risk [13].

Commercial banks are faced with numerous threat and risks from various source of attack. The emergence of e-banking services might not only irritate the occurrence opportunity and the damage of diverse sorts of risks, but also bring new dangers in the domain of monetary offerings and financial services [14].

Regarding to risk management of commercial banks of e-banking services, the western advanced countries is developing the aid through research and practices have accumulated lots of standardized norms and wealthy experiences. However, the practice and research of risk management in Southeast Asia including Malaysia and Singapore commercial banks e-banking services are relatively backward [13].

The e-banking services development for commercial banks primarily based on online internet is facing with critical issues in term of information security because of the vulnerability and complexity of the internet. Normally, several forms of security risks faced by commercial banks are following [13]:

i. Information Tampering: Through a wide spread of technical prospective and means, network attackers generally tamper with, spoil, and compromise the internet software program make the information system failure. Hackers usually tamper with, copy, insert, or delete or transmitting records with the intention to compromise information security integrity.
ii. Data Access Risk: Data access risk is typically the outcome of data modification, deletion, and revision from access to the database server that are coming from unauthorized parties or internal and error conducted by employees and operational mistakes in the commercial banks.
iii. Fake Information: This happened during an attacker is equipped with superior knowledge in hacking, networking, or cryptography skill. They could use false information to deceive other users or become the authorize users of counterfeit.
iv. Online Payment Risk: Online pricing commonly being seemed as the most crucial component proscribing the online trade development of Southeast Asia commercial banks due to there are still quite a number of customers worry and fear about the security level and refuse to apply online transaction.

D. Information Security Risk Audit and Assessment

The elevated demand for Information technology security auditing services underline the significance of conducting the auditing in a most effective and efficient manner. Further, the eye toward IT security audit has arisen due to the following motives which are increasing on expenditure and dependence on IT for commercial organization operations, and a pair of new regulation and professional requirements associated to the audit process of these operations.

One of the major purposes of IT security audits is to provide assurance regarding that a system or automatic procedure is achieving its objectives to management. The focus can be on managements that manage duties or responsibilities on computer based information assets and procedures. In such cases, precise requirements evolved by businesses parties like ISO, AICPA, or PCAOB may additionally help in defining the IT security audit quality [15]. Companies need to make adequate decisions concerning the scope, sources, employees, tools, obligations, activities, strategies, and types of inputs to the IT security audit procedure.

This additionally needs an attention from different attributes that would affect the overall outcome and performance of the IT security audit, but over which they have little to none control. Such attributes usually consist of the availability of key auditee members, architecture, infrastructure, or the organizational structure of an enterprise unit being

Fig. 2. Auditing Phases[16]

Preparation Phases

Everything conducted in advance by relates groups such as audit manager, client, and auditor to ensure that the auditing complies with clients requirements and objectives are during the audit preparation phases. In the preparation stage of an audit process it usually begins with the reason to carrier out the

audit. Auditor begin to analysis all the requirements and objective requested by clients. This phase consist of activities such as staffing the auditing group, and creating the audit project plan or blueprint before the actual implementation of audit [[16].

Performance Phases

[16] states that the performance phases of an audit is commonly defined as the fieldwork. Performance phase is the information collecting stages which covers the time frame starting from arrival at the audit location until the exit meeting. Some of the on-site auditing activities includes meeting with the audit team member, communicate with team members and auditee, understand the fundamental of the process and system controls, analyse whether these controls work through verifying, and on-site information gathering such as firewall, server, network topology, router devices, existing policy, and other. After that, laying down the groundwork for auditing member to conducts the audit process such as penetration test on organization parameters, reviewing or enhances the existing IT policy, analysis the strength of access control from both technical based and administrative based. The auditing process can be done either internally or externally. Lastly, analyse the audit results to prepare for the next phases of audit which is Reporting phases [16].

Reporting Phases

The objective for audit report is to address the outcomes of the audit investigation. Audit report ought to offer accurate and clean effective information as a useful management resource in addressing vital organizational problems. Activities execute on this phases are writing audit results, sharing audit results, and handling with barrier to audit remediation.

Follow-up Phases

After that, an audit closure and follow-up will be carrier on to further enhance or correct any mistakes during the auditing report. Lastly, as according to ISO Standard 19011, clause 6.7 of ISO Standard 19011 continues by stating that verification of follow-up actions may be part of a subsequent audit as it is part of the building an ongoing audit programs. And also clause 6.6 states that "The audit is completed when all the planned audit activities have been carried out, or otherwise agreed with the audit client" In the end, the audit procedure is considered cease when evaluation and follow-up actions are completed or the document of report is issued by the lead auditor [16].

IV. MODEL-DRIVEN SOFTWARE ENGINEERING

During the creation process, the modeling result is mostly a version of the system that explains the surrounded environment and the system for a particular motive. A proper way toward this interest is being refers as conceptual modeling. The model is gathering and collecting the critical components for the motive of assembling the system, designing, understanding, build, deploying and description of the overall view of the system is the essential step to creation process [17].

Variety types of models which are organized collectively and display these models to guarantee the efficiencies in the developed system are being used by driven model. On this undertaking project, a model-driven approach is used to create a system to structure and manage information security risk management knowledge. The model-driven engineering method consists of three kinds of concepts which is standards models, meta-models, and model according to [18].

A. Model

Model is a summary illustration of the real world and is used to assist managing complex of the sector. Researcher also characterised the model as an external and explicit illustration as being seen and define by the people that desire to utilise the model to recognize, control, manage, and modify that a part of fact [18]. Commonly, construct within the extensive areas and model expresses the structure starting from engineering, science, philosophy, arithmetic, management, scientific and other fields. It also have a causal connection is good for reality [19].

According to Quaziet knowledge, layout of next systems to recognize the complex structures and minimize the complexity through decomposing each of them accordingly into smaller pieces and models are supporting the designers within the analysis. Then again, models deliver the designers an opportunity for an excellent communications that force to standard understanding among expertise which may also serve as a mechanism files such as ISO standard [20]. Relationships enable to distinguish the links between entities and a concept or idea distinguishes entities domain [21]. A model normally includes factors like standards and relationships. It has been categorized the models that associated to information systems areas as following [21]:

i) Dynamic or static that static representation of the behavioral aspects of models and system.
ii) Passive and active model which passive is independent of its domain and active is living model.
iii) Executable and viewable models which communicate review of the system on the design and analysis stage.
iv) Conceptual versus data model such as laws and rules.

The model effectiveness can be accomplish through abstracts and extracts of major concepts efficiently. Different criteria encompass models are reliability, completeness, verifiability, significance, improvement, and cost. Lesser time the modeler spends to functions the model when reliable meaning attached to the principles [22]. The terminologies description and relationship among concepts is not always precise to one discipline, different observer may have vary description and relationships concepts [23].

B. Model-Driven Software Development

The functionality, structure, and architecture of the system is being specify by model-driven development formal models and to be used, Rather then, requiring software developers to use programming language to list up how system is being developed [24]. During a structures system creation process, the developer usually applied model-driven method. Entire software program models have been constructed using particular software program language.

Identifies all the elements that can be described as any domain version have been defined as modeling language (ML). With valid models in terms of organize, ML facilitation is sharing the outcome of the modeling process and it only use the most effective specific symbols that in conformity with the regulations. For example, users can summarize the knowledge and allow it to be easier to solve and share the problems with the use of models as beginning point [25].

Distinctive sorts of modelling language already have evolved for a selection of disciplines consisting of systems engineering understanding. Some of the ML use in organization, statistics management, information management, software program engineering, and computer science process modeling. The well-known and popular modeling language used currently consists of Entity relationship model (ERM), Unified Modeling Language (UML), and Event-driven Process Chains (EPC) [26]. The use of mentioned ML facilitates to identify the structures of system so that stakeholders such as operators, customers, designers, analysts, can have the required knowledge and expertise on the system [27].

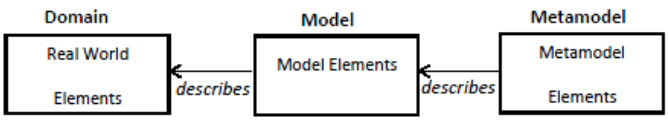

Fig. 3. Relating Real World, Model, and Metamodel Elements [20]

C. Metamodeling Framework

The phrase "Meta" is a common vintage prefix that means "about", due to the discovery that on occasion metamodelling is expressed as modeling about models. Object control institution is the evolver of Metamodelling. Metamodelling has been evolved to create interoperable, reusable, portable software components and activities [28]. [20] mentioned that when comparing against metamodelling and modeling can define that they are equal and have similar activities. Then again, their interpretation is different and their creation is a fundamental state of model.

Actual world system and procedure enable to represent as model. The process of creating different models is during the process modelled and the appropriate description of this modeling is called metamodelling. A metamodelling framework systematically provides recipes for developing, translating, and validating metamodels [20]. Due to that, all ideas and concept that observe for modeling it should also apply for metamodelling. There have been several software program engineers and analysts describing different metamodeling frameworks.

TABLE II. INDICATES LIST OF CURRENT METAMODELING FRAMEWORK[20]

Metamodelling framework	abbreviation	Developer	Year
Object Model for an Object-Oriented System Integration Framework	COOM	Berre	1992
Complex Covering Aggregation	CoCoA	Venable	1993
Nijssen's Information Analysis Method	NIAM	Wintraecken	1993
Common Object Methodology Metamodel Architecture	(COMMA)	Henderson-Sellers and Bulthuis	1996
Object Property Relationship Role	OPRR	Rossi and Brinkkemper	1996
Meta Object Facility	MOF	OMG	2002
Graph Object Property Role Relationship	GOPRR	Rossi et al	2004

The three criteria used to evaluate amongst software engineering metamodelling frameworks that are generality, modeling approach, and pragmatics has been recommended, and by answering question like the development lifecycle of the metamodelling framework has covered until how much and generality can be measure. Second, modeling method which approach used for the effectiveness of other functions are analyzability (ability of internal consistency tests), accessibility (clean to apply, understandable, and comprehensible), assist the complexity of control by using way of growing a couple of abstraction levels (capability to cope with vary levels of abstraction), expressiveness (ability to specify standards and relationships), and outlining the metamodel. Lastly, how the metamodelling has deployed and used is describe by using pragmatics [29].

Metamodelling frameworks have precise path and reason of modeling. For instance, MOF metamodelling primarily focus is regarding the defining information models for metadata. NIAM [30], GOPRR [31] and ER [32] are other metamodel frameworks that have same purpose even as those frameworks are not appropriate for the purpose of simulation-orientated modeling. Kriging [33] is being define as a better choice for simulation purpose. MOF is the chosen framework that adopts and evolves a concomitant procedure for ISRAA in this project. However, the researcher to choose MOF on this study because several benefit is provided by using OMG standard for metadata. It is widely recognition while covering different domains and concord among the standard. In the next section, MOF details discussion will be covered.

D. Metamodeling Development Process

In this journal, MOF metamodeling framework and the standard for metamodeling provided by means of [34] is observed. MOF is largely a meta-metamodel that defines a public method of seizing the diversity of modelling requirements, standards, and interchange constructs which are applied in best driven multimedia engineering. The MOF is described as a framework designed for outlining modelling languages. MOF is based totally on a hierarchical architecture of 4 meta-layers as illustrated in Fig. 4 below.

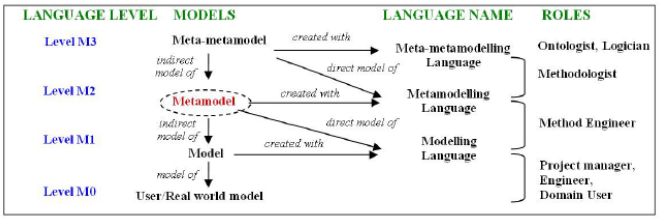

Fig. 4. MOF Framework

MOF is essentially about defining information models for metadata. It makes use of an object modelling framework that is vitally a UML core subset. The primary modeling thoughts in MOF are classes, association, data types and package. The primary benefits of OMG are expansive consented, coverage of countless areas and cohesion amid the common [35].

MOF has 4 layers which are M0, Ml, M2 and M3. It has disparate points of interest on modelling at disparate layers of details. It is harshly hierarchical and at every single given layer below M3 fit in trusted from the layer above.

Each single relied on in every single given layer above M0 can be instantiated on the layer under. M2 level is for the metamodel layer, encompassed of the descriptions of the assembly and semantics of metadata. M1 level is projected for the perfect layer such as example of metamodel, encompassed of the metadata that describe data inside the data layer. The bottom layer M0 is devoted for consumer models such as example of the ideal and additionally yelled as a data layer. In this thesis, M0 layer will cover the data this is ISRAA flawlessly describes at Ml. The ISRAA metamodel is at M2 layer [20].

V. METAMODEL VALIDATION

Metamodel quality measuring is primarily based on how the developed metamodel satisfy the reason and requirement of its creation [36]. Actually, the created metamodel ought to fulfil the needs of the domain practitioners. It also concerned in enhancement the knowledge quality within domain and to make sure potential expert in the domain to validate the metamodel. Metamodel need to be validates in order to fulfil the requirement of expressiveness, completeness, and generality of the artifact. Usually, developer needed to answer how the metamodel is applicable to its real application domain after metamodel is efficaciously created. The developer determined to apply the 2 technique to validate ISRAA metamodel which are face validity and comparison against other models.

VI. RESEARCH METHODOLOGY

A. Operational Framework

Design is a process with lot of ideas and activities by which an artefact is developed and realised [37]. Design Science supports a practical research paradigm researcher that desire to develop of innovative artifacts that enable to solve real world issues. Design Science Research demands for creative innovative and effective artefact for particular domain issues and also the development, application of new design techniques, procedures, and methods is included [38].

Design Science Research is the appropriate approach to develop a trustworthy ISRAA metamodel and therefore it is used to achieve the objective of this research. Design Science Research cycle consist a process of evaluation and repetition against the created artifact. In order to present the artifact to users, the evaluation and construction of the artifact must be properly executed. Evaluate the ISRAA metamodel to assure its usefulness for ISRAA is supreme. In this study, researcher designed the research work into 4 development phases through the methodology of Design Science Research. The four development phases are as follow: Phase 1 Set up the problem relevancy and developing the research problem description, Phase 2 The development and creation of the ISRA metamodel, Phase 3 The validation of the ISRAA metamodel, and Phase 4 The outcome of the developed ISRAA metamodel.

B. Metamodel Validation Techniques

Design Science Research should strictly internally consistent, coherent, defined, formally represented and this is the significance between Design Science Research and other practices of design process [39]. To achieving this, validation for ISRAA metamodel is required. Two validation techniques will be applied:

i) Comparison Against other Models [40]: This technique enable researcher to verify the accuracy of the initial derived concepts and investigate missing concepts from the domain models being investigated in the early development phases of the initial ISRAA metamodel.

ii) Face Validity (Siu *et al.*, 2017): This technique requires the developer to conduct an interview with the expert from the domain. In this research, the expert is Credit Risk Manager from DBS bank Singapore, Risk Manager from Public Bank Malaysia, and IT Support Officer from UOB bank.

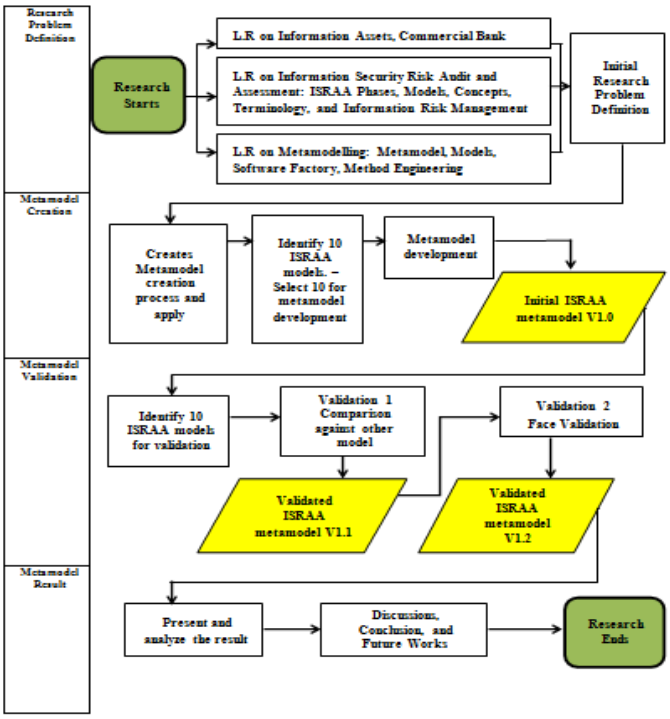

Fig. 5. Research Framework for ISRAA Metamodel

C. Case Study Commercial Bank

The main reason of the development of ISRAA metamodel is to assist in ISRAA model related problems in IT asset of commercial bank domain. Developed ISRAA metamodel can benefits the ISRAA model users in term of contents and comprehensiveness. Besides that, the developed ISRAA metamodel also contributes to users in enable them to choose specific concepts of class in this metamodel to suite their particular situation and environment by following the concept step lists. In order to validate the ISRAA metamodel effectiveness in real world commercial bank domain, a case study related to ISRAA issues is chosen to be a problem to metamodel.

The commercial bank selected for this project case study includes: (i) Public Bank – Public Bank receives Asian banking excellence award from FinanceAsia (Hong Kong-based business publication) [42], (ii) DBS Bank – Euromoney (gives out numerous awards for excellence to firms in many categories, at country, regional, and global levels) Best digital bank award winner Development Bank of Singapore (DBS) Bank [43], and (iii) UOB Bank - Winners of WealthBriefingAsia Singapore Awards 2016 for the Best Private bank Southeast Asia United Overseas Bank (UOB) Bank [44].

The position of personal from these selected banks will consists of managerial level and IT staff (e.g. Branch Manager, Risk Manager, and IT Support Officer). As these banks are relatively one of the largest and popular banks at their own operating countries in Malaysia [45] and Singapore, It is appropriate to select these banks as the project case study to cover a wider scope of commercial bank ISRAA model around Southeast Asia.

VII. ISRAA METAMODEL CREATION

Step 0: Models collection and preliminary domain study. In overall, 20 ISRAA model is gathered from variety type of sources e.g. book, thesis, research paper, online source, conference papers and other. Knowledge source are all collected through public domain models. The phases and common element of ISRAA metamodel have also been familiarized. In order to avoid incompleteness problem, the domain awareness need to be enhance.

Step 1: Identifying sub-sets of models to suit research tasks. For the purpose of initiate metamodeling process and prepare a validation set, 10 ISRAA models have been collected by using model coverage selection criterion to identify each of the model.

Step 2: Extraction of general concepts in models identified in Step 1. Extracted concepts are the ISRAA type independent

Step 3: Shortlisting candidate definitions. A set of general concepts grounded in commonly agreed meaning in ISRAA domain is adopted because of widespread occurrence of any particular ISRAA management definition. Those considered implicit definitions that can be subject to interpretation, a greater weight is given to sources with clearer definitions

Step 4: Reconciliation of definitions. When there is definition of two or more sources are inconsistent. If there is an inconsistency occurring between two or more sources, the concept which has more coherent usage with the rest of the chosen concepts is chosen. Furthermore, to maintained consistent with earlier choices, the common concept definition should be choose and used.

Step 5: Designation of concepts are categorized. This is a standard ISRAA management abstraction corresponding to ISRAA management phases which separate into 4 sets which are preparation, performing, reporting and follow-up. It is common to most of the models that are considered.

Step 6: Identification of relationships within and across preparation, performing, reporting, follow-up relationships and diagram interfacing the categories. The initial version of the ISRAA Metamodel will be the result of this step.

Step 7: Validating the metamodel. face-validation and comparison against other models validation techniques are used to validate the ISRAA Metamodel. The next section will further discuss the development of ISRAA Metamodel Steps 1 to 6.

VIII. CONCLUSION

In the end, commercial bank IT assets technology and infrastructure are evolving hence there may be certain areas that could be unfamiliar to IT auditors whom are accustomed to variety type of IT security auditing models. Due to this reason, ISRAA model must be guided by certain bases that outline the key focus areas to be emphasized on, as compared to the routinal areas which auditors review and analyse during a classic IT security audit.

The second inherent contribution of this study is the development of the comprehensive ISRAA metamodel consisting of the identfied components in the first contribution. The model which illustrates the relationships between the explicit outcome of the model i.e. ISRAA metamodel serves as a guide for auditors to familiarize themselves with the key focus areas for them to further prepare their auditing plan and determine the scope of review prior to commencing a IT assets Information Security Risk Audit and Assessment in commercial bank review for a more enhanced and improved audit processes as a whole.

ACKNOWLEDGMENT

I would like to express my gratitude to family, friends, and mentor providing me the blessing to complete this work. Hence, I am deeply grateful to my supportive and helpful supervisor Dr Siti Hajar Binti Othman and programme coordinator Dr Maheyzah Binti Md Sirat for assisting and guiding me in the completion of this project.

REFERENCES

[1] J. A. Dantas, F. M. da Costa, J. K. Niyama, and O. R. de Medeiros. (2014). Audit Regulation in Banking Systems: Analysis of the International Context and Determining Factors. *Rev. Contab. Finanças*, 25(64), 7-18.

[2] C. Jarko. (2017). Built From Scratch – Creating an Audit Program for a Nonprofit Organization. *Glob. Inf. Assur. Certif. Pap.*

[3] I. Sutton and I. Sutton. (2015). Chapter 13 – Audits and Assessments. *Process Risk and Reliability Management*, 538-579.

[4] T. G. Calderon and J. J. Cheh. (2002). A Roadmap for Future Neural Networks Research in Auditing and Risk Assessment. *Int. J. Account. Inf. Syst.*, 3(4), 203-236.

[5] A. Singh. (2009). Improving Information Security Risk Management.

[6] C. Bao, J. Li, D. Wu, X. Zhu, C. Liang, and C. Liu. (2014). Optimization of Integrated Risk in Commercial Banking based on Financial Statements, *Procedia Comput. Sci.*, 31, 501-510.

[7] Archives. (2017). Identifying Information Assets and Business Requirements.

[8] L. Vilcahuamán, R. Rivas, L. Vilcahuamán, and R. Rivas. (2017). Chapter 5 – Asset & Risk Management Related to Healthcare Technology. *Healthcare Technology Management Systems*, 71-101.

[9] S. N. Institute. (2016). Asset Inventory and Security Management in ICS. *Spain: CertSi Security and Industry Cert*, 2016. [Online]. Available: https://www.certsi.es/en/blog/asset-inventory-and-security-management-ics. [Accessed: 01-Dec-2017].

[10] C. S. F. Ho and N. I. Yusoff. (2009). A Preliminary Study on Credit Risk Management Strategies of Selected Financial Institution in Malaysia. UKM.

[11] B. Y. Yee and T. M. Faziharudean. (2010). Factors Affecting Customer Loyalty of Using Internet Banking in Malaysia. *J. Electron. Bank. Syst.*, 21.

[12] Investopedia. (2017). Commercial Bank. 2017. [Online]. Available: https://www.investopedia.com/terms/c/commercialbank.asp. [Accessed: 01-Dec-2017].

[13] L. Bo and X. Congwei. (2017). E-commerce Security Risk Analysis and Management Strategies of Commercial Banks. *Information Technology and Applications, 2009. IFITA'09. International Forum on*, 1, 423-425.

[14] Q. Chi and W. Li. (2017). Economic Policy Uncertainty, Credit Risks and Banks' Lending Decisions: Evidence from Chinese Commercial Banks. *China J. Account. Res.*, 10(1), 33-50.

[15] D. Stoel, D. Havelka, and J. W. Merhout. (2012). An Analysis of Attributes that Impact Information Technology Audit Quality: A Study of IT and Financial Audit Practitioners. *Int. J. Account. Inf. Syst.*, 13(1), 60-79.

[16] J. P. Russell. (2013). What is Auditing? *ASQ Quality Press*, 2013. [Online]. Available: http://asq.org/learn-about-quality/auditing/. [Accessed: 01-Dec-2017].

[17] S. S. Alhir. (2003). Understanding the Model Driven Architecture (MDA).

[18] T. Levendovszky, B. Rumpe, B. Schätz, and J. Sprinkle. (2010). 9 Model Evolution and Management. *Model-Based Engineering of Embedded Real-Time Systems*. Springer. 241-270.

[19] U. Aßmann, S. Zschaler, and G. Wagner. (2006). Ontologies, Meta-models, and the Model-Driven Paradigm. *Ontologies for Software Engineering and Software Technology*, C. Calero, F. Ruiz, and M. Piattini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg. 249-273.

[20] S. H. Othman. (2012). Metamodelling Approach for Managing Disaster Management Knowledge. University of Wollongong.

[21] J.-P. Van Belle. (2004). A Proposed Framework for the Analysis and Evaluation of Business Models. *ACM Digit. Libr.*, 210-215.

[22] J. M. Sprinkle and G. Karsai. (2003). Metamodel Driven Model Migration. Vanderbilt University.

[23] A. Gharedgahli. (2003). Design of a Generic Metamodel for Fieldwork Data Management. The International Institute for Geo-information Science and Earth Observation,

[24] C. Atkinson and T. Kuhne. (2003). Model-driven Development: a Metamodeling Foundation. *IEEE*, 20(5), 36-41.

[25] T. Weilkiens. (2011). *Systems Engineering with SysML/UML: Modeling, Analysis, Design*. Morgan Kaufmann.

[26] A.-W. Scheer, O. Thomas, and O. Adam. (2005). Process modeling using event-driven process chains, *Process. Inf. Syst.*, 119-146.

[27] M. Völter, T. Stahl, J. Bettin, A. Haase, and S. Helsen. (2013). *Model-driven Software Development: Technology, Engineering, Management*. John Wiley & Sons,

[28] J. Sprinkle, B. Rumpe, H. Vangheluwe, and G. Karsai. (2010). 3 Metamodelling. *Model-Based Engineering of Embedded Real-Time Systems*. Springer. 57-76.

[29] A. Sturm. (2009). How to Choose A Metamodeling Approach. *The Knowledge Industry Survival Strategy: Initiative Workshop of the International Conference on Object Oriented Programming, Systems, Languages and Applications (OOPSLA)*. New York, NY.

[30] M. Lombard and P. Lhoste. (2008). Information Modelling Framework for Knowledge Emergence in Product Design. *Global Design to Gain a Competitive Edge*. Springer, 241-250.
[31] M. Rossi, B. Ramesh, K. Lyytinen, and J.-P. Tolvanen. (2004). Managing Evolutionary Method Engineering by Method Rationale. *J. Assoc. Inf. Syst.*, 5(9), 12.
[32] D. J. Pigott and V. J. Hobbs. (2011). Complex Knowledge Modelling with Functional Entity Relationship Diagrams. *VINE*, 41(2), 192-211.
[33] W. C. M. Van Beers. (2005). Kriging Metamodeling for Simulation. Tilburg University, School of Economics and Management.
[34] OMG. (2002). Meta Object Facility MOF Specification.
[35] S. Cook. (2004). Domain-Specific Modeling and Model Driven Architecture, *MDA J*.
[36] P. Bermell-Garcia. (2007). A Metamodel to Annotate Knowledge based Engineering Codes as Enterprise Knowledge Resources. *Springer Link*, 4.
[37] M. M. Andreasen, N. Wognum, and T. McAloone. (2002). Design Typology and Design Organisation.
[38] N. Cross. (2007). Editorial Forty Years of Design Research.
[39] A. Hevner and S. Chatterjee. (2010). Design Science Research in Information Systems BT - Design Research in Information Systems: Theory and Practice, A. Hevner and S. Chatterjee, Eds. Boston, MA: Springer US. 9-22.
[40] J. P. C. Kleijnen and D. Deflandre. (2006). Validation of regression metamodels in simulation: Bootstrap approach. *Eur. J. Oper. Res.*, 170(1), 120-131.
[41] B. W. M. Siu, C. C. Y. Au-Yeung, A. W. L. Chan, L. S. Y. Chan, K. K. Yuen, H. W. Leung, C. K. Yan, K. K. Ng, A. C. H. Lai, S. Davies, and M. Collins. (2017). Validation of the Security Needs Assessment Profile' for Measuring the Profiles of Security Needs of Chinese Forensic Psychiatric Inpatients, *Int. J. Law Psychiatry*, 54, 61-66.
[42] Y. Yong. (2017). Public Bank Receives Asian Banking Excellence Award from Finance Asia. *theedgemarkets.com*, 2016. [Online]. Available: http://www.theedgemarkets.com/article/public-bank-receives-asian-banking-excellence-award-financeasia. [Accessed: 01-Dec-2017].
[43] J. Bloomberg. (2016). How DBS Bank Became The Best Digital Bank In The World By Becoming Invisible. *Forbes*, 2016. [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2016/12/23/how-dbs-bank-became-the-best-digital-bank-in-the-world-by-becoming-invisible/#1dbdbcfb3061. [Accessed: 01-Dec-2017].
[44] T. Burroughes. (2017). Winners of Wealth Briefing Asia Singapore Awards 2016. *Wealth Briefing Asia*, 2016. [Online]. Available: http://www.wealthbriefingasia.com/article.php?id=169365#.Wkc0J1WWbcd. [Accessed: 01-Dec-2017].
[45] A. Pakirisamy. (2017). Public Bank Closing in on Maybank for Top Bank Title, *The Star Online*, 2016. [Online]. Available: https://www.thestar.com.my/business/business-news/2016/11/02/public-bank-closing-in-on-maybank-for-top-bank-title/. [Accessed: 01-Dec-2017].