TÉCNICO LISBOA

Information Security Incident Management: Supporting Systemic Corrective Actions using Enterprise Architecture

Fábio Duarte Gonçalves Lourenço

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisors: Prof. André Ferreira Ferrão Couto e Vasconcelos

Prof. Miguel Leitão Bignolas Mira da Silva

Examination Committee

Chairperson: Prof. João Emílio Segurado Pavão Martins

Supervisor: Prof. André Ferreira Ferrão Couto e Vasconcelos

Member of the Committee: Prof. Miguel Nuno Dias Alves Pupo Correia

November 2017

Acknowledgements

Thanks to the supervisors for the guidance provided, to DemoCorp for allowing the demonstration present in this document and for the time spent to validate the work, to Link Consulting for providing a license for EAMS during the period of this research, and to my parents and girlfriend for the support provided during this research.

Resumo

Independentemente do investimento na Segurança da Informação (SI), as organizações não estão imunes a incidentes de segurança da informação. Assim sendo, é fundamental que estas aprendam com o seu historial de incidentes e executem ações corretivas para prevenir incidentes futuros relacionados. No entanto, as organizações têm dificuldade em realizar estas ações.

Nesta investigação, propomos uma metodologia que usa Arquitetura Empresarial (AE) para suportar ações corretivas sistémicas no âmbito da Gestão de Incidentes de Segurança da Informação (GISI). Para isso, propomos também a extensão do meta-modelo do ArchiMate para incluir incidentes de SI e o uso do EAMS como ferramenta de gestão de AE. A metodologia proposta consiste em cinco fases que incluem a: i) definição do âmbito, ii) modelação da AE, iii) utilização da AE para suportar a aprendizagem em ciclo duplo e a comunicação, iv) utilização da EA para suportar ações corretivas sistémicas, e v) identificação e análise de riscos de SI.

Para demonstrar esta proposta, a metodologia foi testada com os dados de uma organização, com o nome fictício de DemoCorp, que tem dificuldades em aprender com os incidentes e a realizar correções sistémicas. Para avaliar, a metodologia proposta foi comparada com o processo atual e com uma outra alternativa. Com esta avaliação, foi possível identificar vantagens relativamente ao processo de GISI atual a médio e longo prazo, apesar de ser necessário um maior esforço inicial.

A metodologia proposta oferece uma nova abordagem para satisfazer as necessidades das organizações, descrevendo como obter vistas relevantes dos ativos utilizando AE para melhorar as capacidades corretivas, e suportando a aprendizagem relativa à GISI e a comunicação com outras partes interessadas.

Palavras-Chave:

Gestão de Incidentes de Segurança da Informação, Arquitetura Empresarial, ArchiMate, EAMS, Gestão de Riscos de Segurança da Informação, Aprendizagem em Ciclo Duplo

Abstract

Organisations are not immune to information security incidents regardless how much they spend in information security (IS). Considering this, it is fundamental to ensure that organisations learn from the past incidents and perform corrective actions to avoid future related incidents. However, organisations have difficulty performing these actions.

In this research, we propose a methodology that uses Enterprise Architecture (EA) to support systemic corrective actions in Information Security Incident Management (ISIM). To achieve this, we also propose the extension of ArchiMate's metamodel to include IS incidents, and the usage of EAMS as an EA management tool. The proposed methodology consists in five phases that include: i) scope definition, ii) EA modelling, iii) using EA to support double-loop learning and communication, iv) EA usage to support systemic corrective actions, and v) IS risk identification and analysis.

To demonstrate this solution, the methodology was tested with the data of an organisation, with the alias of DemoCorp, that has issues performing systemic corrective actions. To evaluate, the proposed methodology was compared to the process that DemoCorp currently follows as well as with one other alternative. With this evaluation, it was possible to identify relative advantages to the current ISIM process in medium and long term, despite a greater initial effort.

The proposed methodology provides a new approach to fulfil organisational needs by describing how to obtain relevant views of the assets using EA to improve organisation's corrective capabilities, and supporting ISIM learning and communication with other interested parties.

Keywords: Information Security Incident Management, Enterprise Architecture, ArchiMate, EAMS, Information Security Risk Management, Double-Loop Learning

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Term
1NF	First Normal Form
2NF	Second Normal Form
ADTree	Attack-Defence Tree
API	Application Program Interface
BPMN	Business Process Modelling Notation
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
DSL	Dynamic Security Learning
DSRM	Design Science Research Methodology
EA	Enterprise Architecture
EAMS	Enterprise Architecture Management System
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
IRT	Incident Response Team
IS	Information Security
ISIM	Information Security Incident Management
ISIRT	Information Security Incident Response Team
ISMS	Information Security Management Systems
ISRM	Information Security Risk Management
ITIL	Information Technology Infrastructure Library
UPS	Uninterruptible Power Supply

Glossary

Term	Definition	Source(s)
Availability	Property of being accessible and usable upon demand by an authorized entity	[1]
Chief Information Security Officer	Chief Information Security Officer. Senior-level executive within an organisation responsible for establishing and maintaining programs to ensure information assets are adequately protected.	[2]
COBIT 5 for Information Security	COBIT 5 for Information Security provides guidance for information security professionals and other interested parties at all levels of the enterprise.	[3]
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes	[1]
Information Security Incident Management	Processes for detecting, reporting, assessing, responding to, dealing with	[1]
Integrity	Property of accuracy and completeness	[1]
ITIL Version 3 Service Operation	ITIL Version 3 Service Operation provides best practice advice and guidance on all aspects of managing day-to-day operation of an organisation's IT services.	[4]

1. Introduction

The world is facing the information age which means an economy based on information that is supported by computers and networks [5]. In the current economy, information and knowledge distribution is the major source of wealth [6], therefore, it is important to understand the related challenges, particularly regarding information security (IS).

IS is commonly addressed considering confidentiality, integrity and availability, known as the CIA Triad. When an event with a negative impact affects at least one of the CIA properties, this event is considered an IS incident. According to Ahmad et al. “it is inevitable at some stage that organisations will suffer an IS incident. Such an incident may result in multiple negative impacts, such as loss of company reputation and customer confidence, legal issues, a loss of productivity and direct financial loss” [7]. IS incidents’ consequences may be very high (e.g., a theft of intellectual property on the flagship product of a company may be translated into significant amounts of money lost).

Considering this, it is fundamental to have adequate Information Security Incident Management (ISIM), to try to reduce the impact of those incidents by reducing their probability and consequences. To do so, a possible approach is to use the information obtained from IS incidents and perform corrective actions in the system that will act as measures to prevent future IS incidents, these corrections are called systemic corrective actions.

Despite the value of systemic corrective actions being perceived by organisations, organisations have difficulty performing these actions in the context of IS incidents [7], [8]. Not performing these actions may lead to an inefficient and ineffective ISIM due to the inexistence of continuous improvement and ineffective communication with other teams due to lack of understanding about the incidents.

To solve this problem, we propose to use a methodology supported by enterprise architecture (EA) to improve learning capabilities regarding ISIM and support systemic corrective actions. To achieve this, we also propose the extension of ArchiMate’s metamodel to include IS incidents, and the usage of EAMS as an EA management tool.

To evaluate this proposal, the methodology was tested with the data of an organisation, designated as DemoCorp in this document from now on. This organisation is currently facing issues both learning from incidents and performing systemic corrective actions related with IS incidents. The proposed methodology was tested to understand its usability as well as the benefits that it brings.

This research contribution consists in a methodology to support ISIM using EA and an existing tool to manage EA and ease the effort to maintain it. For organisations, this research presents an alternative

and/or complement to their ISIM process that is explained step by step and offers the necessary knowledge to take advantage of EA as an ISIM tool.

This document structure aims to be aligned with the research method that was followed, Design Science Research Methodology (DSRM). With that in mind, in Section 2 the research methodology is explained. In Section 3 the research problem is introduced and detailed and the research questions are defined. In Section 4 the literature is analysed to understand the current knowledge and practices regarding ISIM. Section 5 presents previous research that is relevant to solve the identified problem. Section 6 presents the solution to solve the stated problem. Section 7 presents a demonstration of the proposed solution. In Section 8 the proposed solution is evaluated. Section 9 presents the details about how this research was communicated, the contributions, limitations of this research and possible future work.

2. Research Methodology

The methodology used in this research was the Design Science Research Methodology (DSRM) [9] [10] [11] in order to have some guidance along the research process.

DSRM is a set of research techniques that aims to produce artefacts capable of improving information systems that present some innovation. The solutions produced tend to have a pragmatic nature in the sense that they can be applied to solve real-world problems [12]. The DSRM process model consists in six activities that follow a nominal process sequence as shown in Figure 1. This process presents iterations that are useful in the sense that it implies that the solution is refined after performing an evaluation using the organisation and reflect about what can be improved, or by communicating the results of the proposal and receiving feedback from peers in this research area.

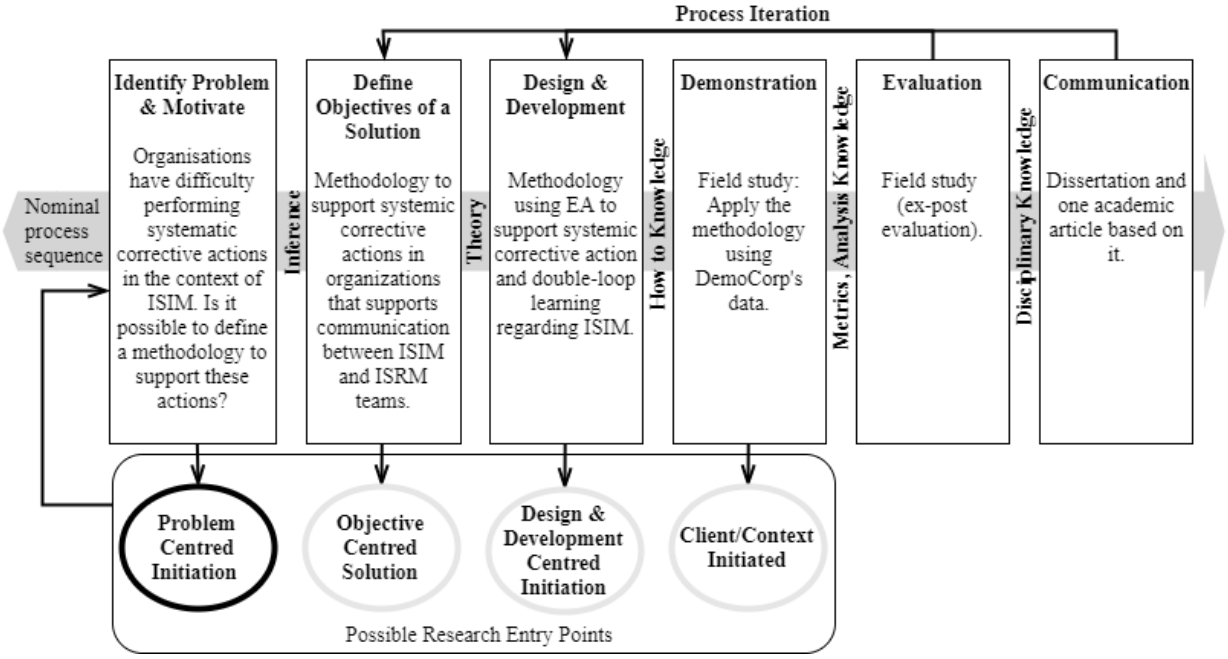


Figure 1 - DSRM mapped to the presented research (adapted from [10]**).**

With this said, this methodology is adequate for the scope of this research since the problem is related with information systems and the idea is to bring innovation regarding ISIM. The pragmatic nature can be confirmed by the fact that this research was tested in an organisation with the expectation of improving their practices regarding ISIM. Despite this pragmatic nature, the research problem was identified in literature, as so it is considered a problem centred initiation [10].

This document counts with two types of artefacts: abstract and material, according to the definitions used in [11]. The abstract artefact in this document is a methodology as can be seen in section 6. The material artefact is an instantiation of the methodology. The instantiation was performed with

DemoCorp's data and a simplified simulation of it is also present in this document in section 7.1 to clarify the proposal.

The structure of this document is based on DSRM structure to be coherent with the research methodology used. Therefore, it is possible to map the sections in this document into DSRM activities.

Sections 3 (Research Problem), 4 (Theoretical Background), and 5 (Related Work) detail the problem identification and motivation. Section 6 (Solution) details the solution objectives as well as the design and development of a methodology to support systemic corrective actions. Section 7 (Demonstration) details how the methodology was demonstrated with DemoCorp's data. Section 8 (Evaluation) details which were the criteria used to evaluate the proposed solution and the corresponding evaluation. Section 9 (Conclusion) presents the conclusions obtained with this research, describes how this research was communicated, its contributions, limitations and future work.

3. Research Problem

Problem identification, as seen in section 2, is part of the DSRM. As so, defining it clearly is fundamental to produce appropriate results. In this section, the problem and the related research questions are defined. After that the problem consequences are explained.

The identified problem is that:

Organisations have difficulty performing systemic corrective actions in the context of ISIM [7], [8]**.**

This problem leads to the following research questions:

- Is it possible to define a methodology to support systemic corrective actions in ISIM?
- How can systemic corrective actions regarding ISIM be used by Information Security Risk Management (ISRM)?

These questions are interconnected as illustrated in Figure 2**.** This figure summarizes the context of this research, the major problem as identified before is that organisations have difficulty performing systemic corrective actions. This happens due to the lack of methodologies and tools available to support these actions, despite the existence of frameworks such as COBIT 5 for Information Security and IS standards they do not provide a step by step methodology or process to support systemic corrective actions. Furthermore, the tools and methodologies that address this issue should provide guidance on how these corrections should be communicated and mechanisms to support communication between teams since in the context of IS, the information of what has changed is relevant for ISRM team for example.

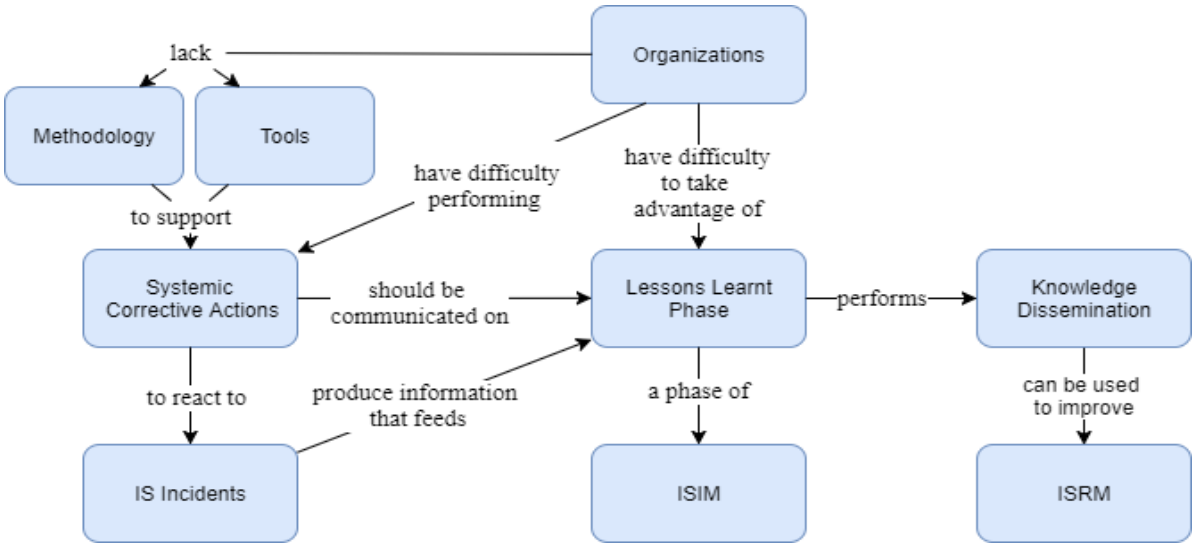


Figure 2 - Problem diagram.

As seen in [7], [8] and also in DemoCorp, organisations have difficulty performing systemic corrective actions despite recognizing their importance. Systemic corrective actions requires questioning the system and its core, fundamental principles [7] [13]. These actions imply the correction of system's vulnerabilities at their different levels according to the definition of vulnerability provided by [14]. These levels include the system's design, implementation, or operation and management.

Not performing these actions may lead to an inefficient and ineffective ISIM due to the inexistence of continuous improvement. Performing only direct corrective actions instead of systemic corrective actions, limits not only ISIM capabilities but also IS as a whole, since the continual improvement stated in [15] would be limited in terms of input information, affecting also ISRM for example.

ISRM benefits from systemic corrective actions since they reduce the existing risk levels and the learning required to perform these actions may be used for future risk analyses and treatment. However, for that to happen it is necessary the existence of proper communication and knowledge dissemination between teams, particularly the ISIM and ISRM teams. According [16], when it comes to IS and incident management there are symptoms of unsatisfactory communication and collaboration, therefore this issue should be addressed as a way to improve IS.

4. Theoretical Background

In this section ISIM is introduced as presented in literature, according to the major standards, frameworks and academic papers that are relevant for ISIM, computer security incident management, and incident management in general. The generic incident management practices and computer security incident management are analysed to contextualize the existing problem in ISIM.

4.1. Base Concepts

In this section, the concepts required to analyse ISIM are briefly explained.

4.1.1. Data and Information distinction

To state it simply, data consists in factual content. Data is a sequence of symbols with meaning [14] that by itself does not add value to an organisation. In order to extract value from that, it is necessary to organize data into categories that make sense for a determined purpose and this is called information [6].

Information is an important asset for organisations and it can exist in many forms: printed or written in paper, electronically in films or audio or even in human resources, available through conversations [3]. Considering the importance that information has, ensuring its security should be a concern for organisations.

4.1.2. Information Security

IS ensures that information's CIA properties are preserved. CIA stands for confidentiality, integrity and availability [3]. Confidentiality is the property related with the guarantee of protection from disclosure to unauthorized parties, integrity is associated to the protection from unauthorized modifications and availability is the property where the concerns regarding the protection from interruptions in access for the authorized parties are discussed [3].

Other properties such as authenticity, accountability, non-repudiation and reliability can be involved as well [1], however along this document only CIA properties will be considered since they are the ones that present more agreement across the bibliography used.

To address the concepts related with IS, the standards of the following organisations were used, i) International Organisation for Standardization (ISO), ii) International Electrotechnical Commission (IEC),

iii) National Institute of Standards and Technology (NIST), which is an organisation with the mission of promoting the innovation partly by advancing standards.

From ISO and IEC, there is the ISO/IEC 27000:2014, which is the standard that provides an overview of Information Security Management Systems (ISMS), terms and definitions that are used in ISO standards related with ISMS; ISO/IEC 27001 that specifies the requirements to implement, maintain and improve an information security management system in the context of an organisation; and ISO/IEC 27035 that provides a structured and planned approach to manage IS incidents along their lifecycles.

From NIST, there is the NIST 800-61 that helps to handle computer security incidents by providing a set of recommendations for the preparation of incident response.

Adding to these organisations, Information Technology Infrastructure Library (ITIL), which is composed of a set of concepts and good practices regarding service management, development and operation in IT was also used to show how concepts with the same name vary in their meaning with that clarify the concepts used along this dissertation.

4.1.3. Event Distinction

According to ITIL Version 3 Service Operation, an event is “a change of state that has significance for the management of a Configuration Item of a configuration or IT Service” [4].

In the context of IS an event has a different meaning. It is an “identified occurrence of a system, service or network state that indicates a possible breach in IS policy or failure of controls or a previously unknown situation that may be security relevant” [1]. NIST has a definition of event that is contained in the ISO/IEC definition since it is simply stated as being any observable occurrence in a system or network [17]. NIST scope of event is limited by computer security however it is important to be considered since IS requires computer security.

This differences in event definition lead to later divergences in the scope of the incidents that may be identified as explained in 4.1.4.

4.1.4. Incident and IS Incident Definition

In the context of a service operation and according to ITIL Version 3 Service Operation, an incident is an unplanned interruption of an IT service, a reduction in its quality or a failure of a configuration item that has not affected the system yet [4].

In computer security, an incident “is a violation or an imminent threat of violation of computer security policies, acceptable use policies, or standard security practices” [17].

Regarding IS, an incident is a “single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security” [1].

These definitions may lead to thinking that these incidents refer to the exact same thing and therefore an incident would always be an IS incident, however, this is not true because of the incident dependence to the event definition of ISO/IEC 27000:2014. Considering this, an incident may not be considered an IS incident, (e.g., in the case of a web service that is used only to perform some calculation, if it is down, it may interrupt one IT service and therefore be considered an incident (as defined in ITIL Version 3 Service Operation) but it does not compromise any security policies and it is not security relevant, so it is not considered as an IS event and consequently not an IS incident.

Despite the fact that computer security and IS incidents are concerned with the confidentiality, integrity and availability of data [18] or information [1], computer security’s scope is limited to computer related incidents. Therefore, these incidents are contained in IS incidents. An example of an IS incident that is not a computer security incident is paper documentation theft, it may affect availability and confidentiality of information but it is not computer related.

These incidents may be deliberate or accidental [19]. IS deliberate incidents may be related with hackers, however they are not limited to them, since an employee with malicious intentions may be able to harm a system on purpose with his own privileges. On the other side, accidental incidents may happen due to human error or acts of nature [19].

4.1.5. Incident Management Overview

Incident Management is, according to ITIL Version 3 Service Operation, the process associated with the management of incidents’ lifecycle and its primary objective is to return the IT service to customers as quickly as possible [4]. However, in IS context, the focus of incident management is to ensure that the impacts from IS being compromised are minimised. Therefore, ISIM differs from (service) incident management and in the next sections ISIM will be further detailed.

4.2. Information Security Incident Management

IS policies or controls may not guarantee total protection of information, information systems or networks. These remaining vulnerabilities may lead to ineffectiveness of IS and possibly and consequently lead to related incidents. Therefore, there is the need to reduce the impacts that such incidents may bring to an organisation. To reduce them there are four primary steps: i) stop and contain, ii) eradicate, iii) analyse and report, and iv) follow up. Besides these steps, preparation is mandatory and this standard provides guidance on how to prepare these incidents [17] [19].

Handling incidents with a well-planned approach helps to increase efficiency regarding the detection, assessment and response but also to improve incident management, by using as input the wisdom that an incident may provide. This approach is expected to provide benefits such as the improvement of overall IS, the reduction of adverse business impacts, improvement of IS risk assessment and management, and the improvement in the material for IS awareness training [19], for example. ISIM's objective is to reduce the impact that incidents may have in an organisation by reducing the probability and the consequence of the incidents [19]. To achieve this, incident management aims to determine the most adequate way to respond to the incidents [17] [19]. With this objective, it should be guaranteed that IS incident response is planned and systematic [19].

Regarding ISIM, it is important to distinguish between what is an incident and an event [18]. The definitions are already clarified in the previous sections, however the distinction between them may not be obvious, as so it is part of ISIM's "Assessment and Decision" phase [19].

The standards are not homogeneous in terms of which are the phases that compose ISIM. Some standards and frameworks consider incident management as a reactive process since a planning phase is not part of it [4] [20]. Others have an explicit phase for planning and therefore use a more proactive approach this is the case of [17] [19]. Regarding the learnings that can be extracted the standards and frameworks once again define with different granularity what should be performed and who should be involved.

There are two standards that are particularly relevant for ISIM, ISO/IEC 27035 and NIST 800-61. ISO/IEC 27035 provides guidelines for ISIM while NIST 800-61 is focused on computer security incident management, which can be viewed as part of ISIM. Figure 3 presents incident management generalized to include both ISO/IEC 27035 and NIST 800-61. This generalization was performed since the phases of incident management in these two documents present differences. The phases will be further explained below using ISO/IEC 27035 terminology and making the correspondence to NIST 800-61 in the description.

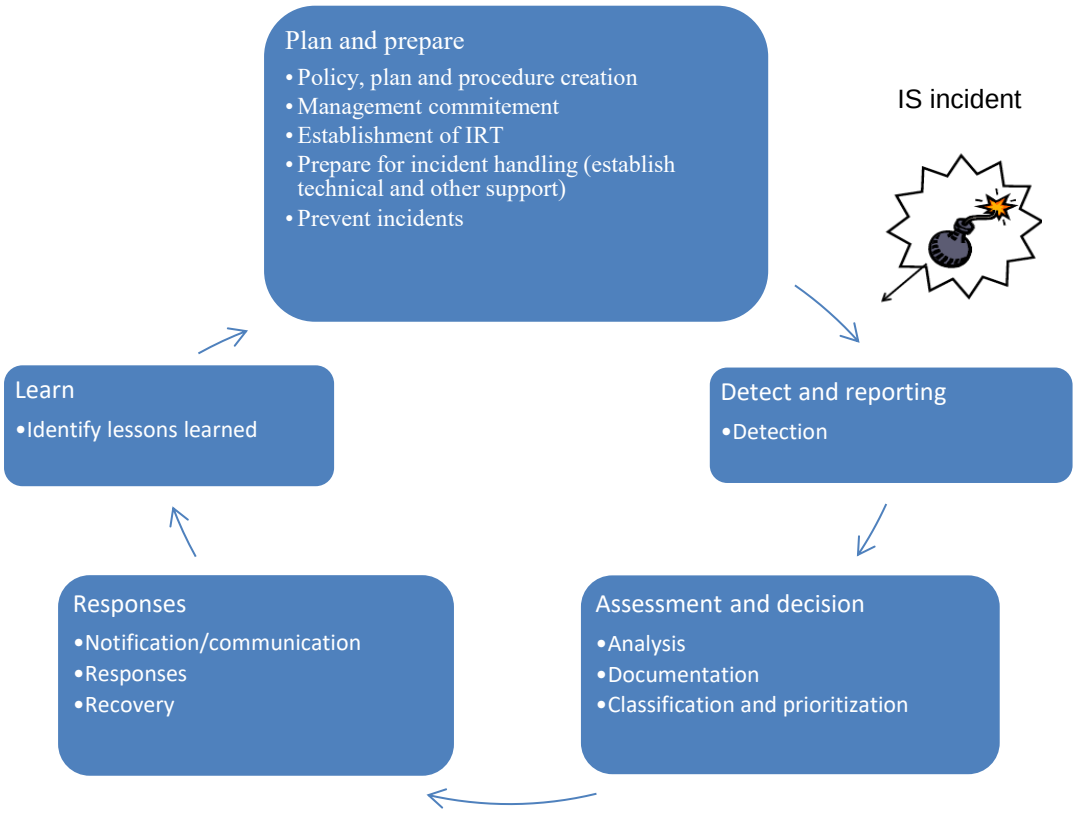


Figure 3 - Incident Management according to ISO/IEC 27035 and NIST 800-61 adapted from [16]**.**

4.2.1. Plan and Prepare

This phase corresponds to Preparation phase in NIST 800-61. In this phase ISIM policies should be established and documented. To create adequate policies, it is important to ensure the commitment from senior management [17] [19]. Amongst other things it is important to establish the IS incident response team, ensure that the people is properly trained and aware regarding IS.

Information Security Incident Response Team

The objective of an Incident Response Team (IRT) in an organisation is to respond to incidents during their lifecycle in a more structured way and consequently doing it more effectively and efficiently [19].

In the context of IS, this IRT is called Information Security Incident Response Team (ISIRT). This distinction relies on the particular set of skills that IS incidents require to handle them and also on the trust required in the ISIRT members [19].

There are other teams with functions that may seem similar to an ISIRT but they differ in the scope and purpose, which is the case of a Computer Emergency Response Team (CERT). CERTs may act at a national level, as it happens in Portugal with CERT.PT which is a service of “Centro Nacional de Cibersegurança”, the Portuguese national cybersecurity centre. CERTs may also act with a broader scope an example of it is CERT-EU, the CERT that acts across the European Union in cooperation with the member states and with specialized IT security companies. There is also the concept of Computer Security Incident Response Team (CSIRT) that refers to the responsible for receiving, reviewing and responding to computer security incident reports and activity [19].

The aim of the ISIRT is to provide to the organisation the capability for assessing, responding to and learning from IS incidents, but also the co-ordination, management, feedback and communication necessary in the context of IS incidents. It is expected from an ISIRT to contribute to reduce the damage associated to IS incidents, physical, monetary or in terms of reputation [19].

Awareness and Training

People are part of ISIM therefore they should be security-aware and properly trained to deal with the organisation’s ISIM processes. It is a requirement to achieve a structured with quality and consequently an effective and efficient ISIM. Incident report is a crucial part of the process and it requires people’s awareness in terms of security but also in terms of the value that an incident report may bring to the organisation [19]. Lessons learned from previous incidents should be shared to clarify how user action may affect the organisation. The improvements in user awareness are expected to reduce the frequency of incidents [17] [21].

4.2.2. Detection and Reporting

This phase corresponds to the detection part of NIST’s “Detection and analysis” phase [17] and is concerned with the detection of IS events, collecting information associated with it, and reporting occurrences of security events and vulnerabilities [19].

4.2.3. Assessment and Decision

This phase corresponds to the analysis part of NIST’s “Detection and analysis” phase [17] [19]. The need for this phase relies in the fact that not all the reports are necessarily incidents, they may be false positives [17] [18] [19]. The objective is to determine if the reported events are incidents and in the case of a positive assessment to determine the severity of an incident and the necessary escalation. The chain of custody should be considered during this phase for future analysis [18]**.**

4.2.4. Responses

Responses phase corresponds to NIST's "Containment, Eradication, and Recovery" phase. In this phase, depending on the decisions, the responses may be immediate or not and some may involve IS forensic analysis. The internal resources should be assigned and the external resources should be identified to respond to an incident. Escalation should be performed as required along this phase. The involved parties such as the ISIRT should log the performed activities for later analysis. Electronic evidences should be gathered and stored securely. IS incident or relevant details to internal and external people or organisations should be communicated [19].

When the incident is related with computer security it is important to contain the incident to limit exposure [18] (e.g., avoid connecting a device to a network where an IS incident occurred). Then eradication takes place by trying to identify the root cause of the incident and then eradicating it. Eradication may not be necessary however recovery is. In recovery administrators restore systems to normal operation, they confirm that they are functioning normally and the identified vulnerabilities are remediated [17].

4.2.5. Lessons Learnt

Lessons Learnt correspond to NIST's Post-Incident Activity. In this phase, forensics analysis should be performed as required, the lessons learnt from IS incidents should be identified. IS control implementation should be reviewed and improved as necessary. IS management policies and security risk assessment should also be reviewed and improved according to what was learnt, and the databases should be updated with the events, incidents and vulnerabilities identified.

In this phase, IS incidents may require application of investigation and analysis techniques to capture, record and analyse them, this process is called IS forensics [19].

The knowledge acquired should be shared within a trusted community [19]. Despite the fact that ISO/IEC 27035:2011 not defining the share as mandatory, NIST identifies the importance of sharing information and the coordination between organisations because "the same threats and attacks often affect multiple organisations simultaneously" [17]. Sharing the knowledge regarding security incidents as real value for organisations since if properly managed it lower costs associated of achieving any level of security [22].

External organisations are not the only interested parties, "risk management team and security strategy and policy developers should be formally included in incident information dissemination and could have a greater participation in the casual analysis as well" [7]. Organisations believe that security risks are known and predictable and based on that they assume that security learning is not required. This leads them to be exposed to new ways of exploiting their vulnerabilities. Security risks are unpredictable and therefore learning from incidents is fundamental to achieve a rapid tactical response [23].

4.2.6. ISIM Process Analysis

ISIM activities are well defined and both standards ISO/IEC 27035 and NIST 800-61 identify the need for learning and state that there should be a relation with risk management and even identify some of the activities that should be performed. The mentioned activities include the identification of trends and patterns, areas of concern and the analysis of possible preventive actions that could be taken [19]. However, these standards do not provide insight regarding which tools may be used to support these actions or how the resulting lessons could be effectively communicated between ISIM and risk management teams as advised in [19]. In practice, this means that each time an organisation wants to follow the good practices of ISO/IEC 27035 and/or NIST 800-61, it will need to create a new solution without a reference process or methodology.

4.3. Information Security Risk Management

Risk is the "effect of uncertainty on objectives" [24]. It may be expressed through the combination of the probability of an event and its consequence [3] [24]. Risk management is a set of coordinated activities to direct and control an organisation regarding risk [24].

Incidents can be seen as the output of risk management [25] in the sense that an incident results from inappropriate or lack of controls for a risk. The focus of this research is how to learn from IS incidents and consequently how to support systemic corrective actions. However, other stakeholders may benefit from it such as ISRM teams. ISRM addresses IS risks which are expressed in term of the combination of the consequence of an IS event and the likelihood of its occurrence [26]. ISRM lifecycle is composed by the context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review [26]. Two of these steps have particular value for this research due to the existing relationship with IS incidents, i) risk assessment and ii) monitoring and review. Risk assessment requires the threats obtained from incident review with the objective of using internal experience from incidents [26] but the methodology to obtain these threats is not clear and it requires some insight of the ISIM. Monitoring and review is performed to the risks and their components to identify if there are changes. One of the mentioned aspects that should be continually monitored are the IS incidents [24].

Despite the fact that ISO/IEC 27005 [26], the standard that provides guidelines for ISRM, states the need for monitoring IS incidents and IS incidents importance in risk assessment, the methodology to enable their usage for ISRM is not defined. In this research, considering the needs of ISRM it is useful to have a common terminology between ISIM and ISRM to enable a more effective and efficient communication between these teams and consequently improve what can be learned from IS incidents as well as improve ISRM by ensuring that ISRM team knows what is done in terms of ISIM (e.g., which incidents occurred, how they impacted the organisation, how they were solved).

5. Related Work

In this section, previous research that may be used to solve the identified problem and answer to the research questions, is analysed. The different approaches to solve the problem are described and the advantages and disadvantages of each approach are stated. The different approaches are also compared in the end of this section to have an overview of the analysed work.

5.1. COBIT 5 for Information Security

COBIT 5 for Information Security provides guidance regarding activities related with IS and the relations between these activities. These relations add value to this research since they reinforce the importance of an appropriate communication between ISIM and ISRM.

COBIT 5 for Information Security has two processes that are closely related with ISIM, “DSS02 - Manage Service Requests and Incidents” and “DSS03 - Manage Problems”. The DSS02 practices, particularly “DSS02.02 Record, Classify and prioritise requests and incidents” output serves as input to APO12 Manage Risk practice “APO12.02 Collect data”. This brings an important link between IS incidents with risk management. The practice “DSS03.05 Manage Problems – Perform proactive management” states a security specific activity that is “Conduct and leverage lessons learned”. However, it does not indicate that this practice is connected with risk management (APO12) as proposed in [7].

COBIT 5 for Information Security guidelines are not enough to perform systemic corrective actions since they do not explain which techniques and tools should be used to learn from IS incidents. There is also no mention on how it should be performed regarding ISIM or ISRM teams since it is only mentioned that data should be gathered and analysed to find trends. Therefore, an organisation that needs or wants to implement a process for systemic corrective actions will find this document insufficient.

5.2. Eramba

Eramba is a web-application that is used for IT governance, risk management, incident management and compliance[1]. Eramba has a free version called community and a paid version called enterprise. Both versions offer a set of automatisms that helps ISIM and ISRM. Eramba is a good start point regarding which information an organisation should monitor to be able to manage IS as it has default data fields that are important in the context of IS and IS certifications such as the ISO 27001 certification. Enterprise version goes further and allows to define custom data fields which are not possible in community version.

Eramba is a useful tool for IT security governance, however, it does not help with systemic corrective actions and it lacks flexibility in the sense that it does not allow customization on how the stored information is showed. Considering this, eramba does not provide a solution for the identified problem as it does not offer a way to be adapted to solve it.

5.3. Single-loop and Double-loop Learning

Incidents have negative impacts, however at the same time they present opportunities to learn about risks [27]. These learnings can be performed at different levels of detail and richness in terms of knowledge acquired.

Single-loop learning is concerned in learning how to fix problems that affect one organisation. It is described as following the rules and ensure that they are followed [28]. Double-loop learning goes beyond as it aims on the reflection on whether the rules should be changed to achieve more efficient processes. To achieve this learning it is necessary to evaluate multiple solutions and understand which one will work better [28]. In Figure 4 it is possible to see a proposal for improving an incident learning system that makes use of double-loop learning. Double-loop learning enables organisations to learn

[1] http://www.eramba.org/about/, accessed on 11/03/2016

effectively with the incidents and mistakes from the past and avoid their repetition. By doing that, double-loop learning provides a strategic and competitive benefit in the longer term [7].

Ahmad, Hadgkiss, and Ruighaver proposed in [7] a learning system with double-loop learning as can be seen in Figure 4. In this system, systemic corrective actions precede double-loop learning and therefore indicates that if an organisation do not perform these actions, the learning obtained from incidents will be limited to how the incident can be corrected and not how related incidents can be avoided in the future.

Despite the importance of the elicitation of systemic corrective actions and double-loop learning, this methodology does not provide insight on how the learning should be performed based on the systemic corrective actions and consequently does not justify the proposed order of activities particularly why double-loop learning should occur after systemic corrective actions and not the opposite since a systemic corrective action requires some previous learning regarding the system.

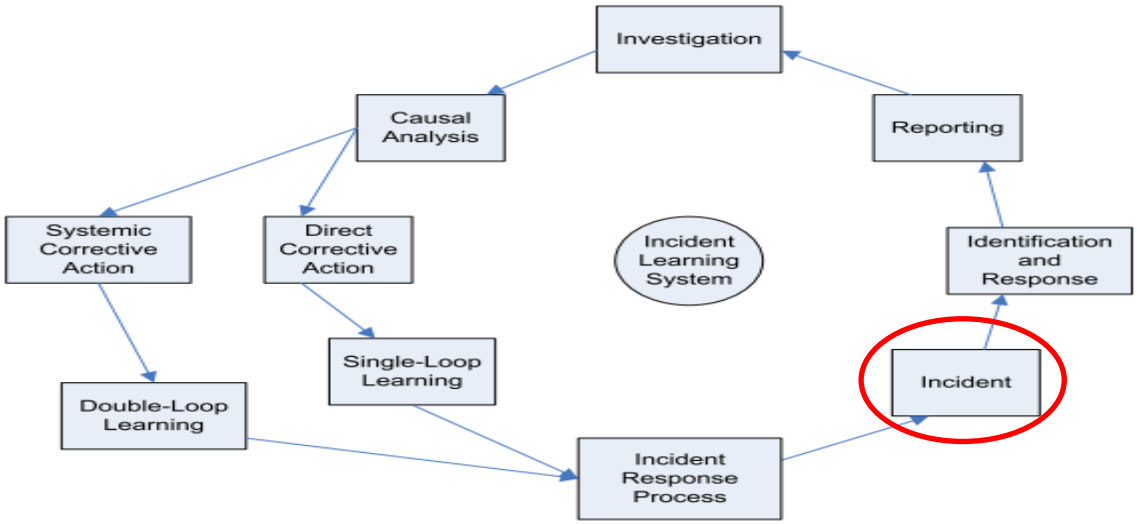


Figure 4 - Incident learning system [7]**.**

5.4. Dynamic Security Learning

Dynamic Security Learning (DSL) is a model that shows how organisations can create novel structures and practices for gaining security insights using the information provided by incidents. It provides an explanation on how double-loop learning regarding IS incidents should occur, it also identifies which stakeholders should be involved and the activities that they should perform related with organisational learning [23]. In Figure 5 it is possible to see succinctly those activities and stakeholders.

DSL importance for this research relies on the fact that it provides an insight on how the learning flow may occur and with it, it is possible to understand the context and the activities that should be supported in the proposed solution. However, it does not define the techniques that should be used as well as a common language for the communication between parties and along the process.

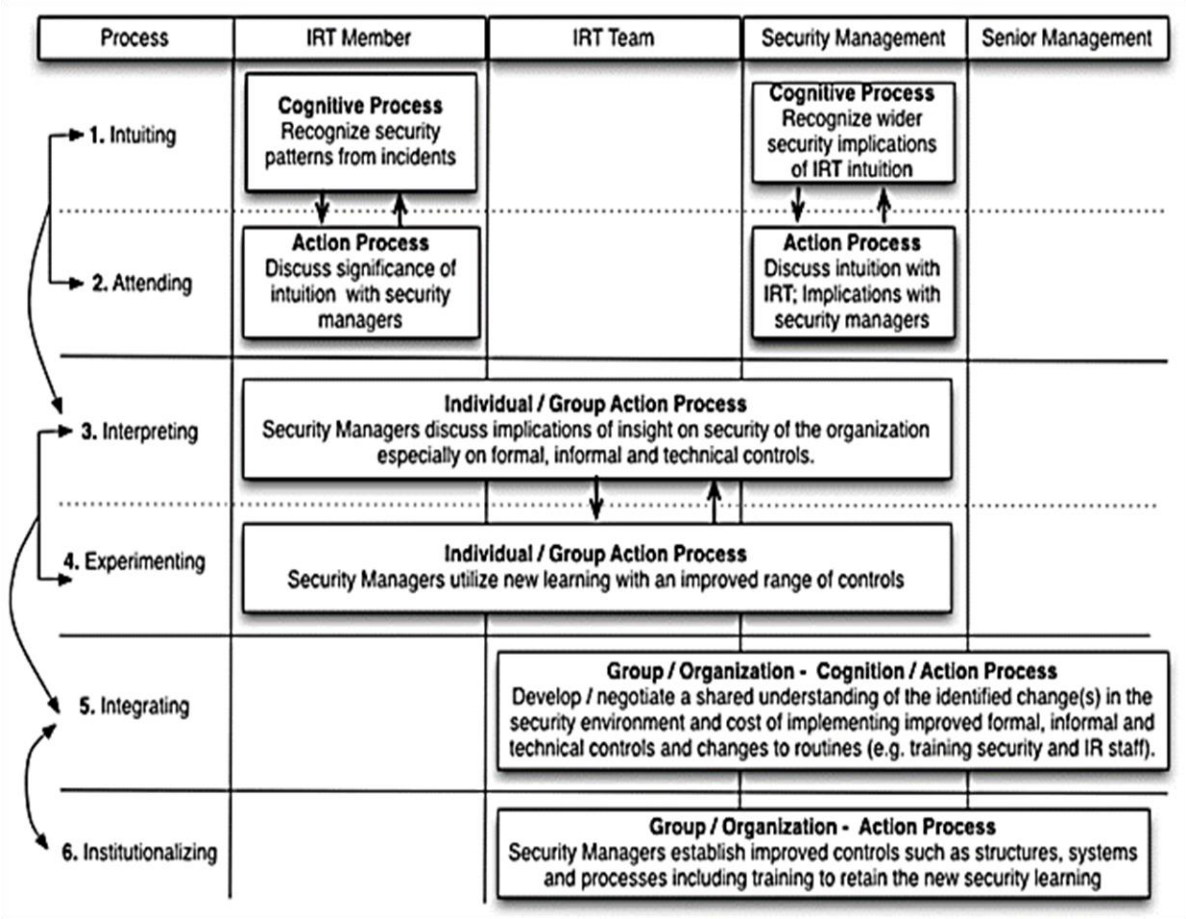


Figure 5 - Dynamic Security Learning (DSL) Process Model [23]**.**

5.5. Attack Vectors

To be able to perform systemic corrective actions, it is necessary to understand the incidents. Considering a deliberate IS incident, it is helpful to analyse the attack in order to eliminate vulnerabilities and implement or adapt the existing security controls [29]. To understand an attack, a representation of attack vectors as described in [29] can be used as a systematic approach.

An attack vector is a path to materialize a threat [29]. This means attacking a target that in an organisational context represents an asset. It is important to note that in order to attack an asset, the path may involve other assets as well as their weaknesses [29].

Attack vectors have two types, ingress and egress. Ingress refers to intrusions while egress refers to network communications going out. In order to perform an attack it is necessary to overcome security controls and for that use an exploit to take advantage of vulnerabilities [18].

Attacks are performed by agents as so it is important to distinguish between which are the threat agent category to allow for refined actions based on agent category. Agents can be distinguished by their skills/expertise, motivations, and privileges to the assets [29]. Appendix A presents the relation between the most common threats and the threat agents involved on them.

Representation of attack vectors are important to understand IS incidents in the context of this research since they present a systemic approach to understand the steps that a threat agent performed to materialize a threat and that is useful to be able to perform direct and systemic corrective actions. However, attack vectors are used for attacks and not all IS incidents correspond to an attack. Attack vectors may also be overwhelming when trying to disseminate knowledge in lessons learned phase. Adding to this, attack vectors do not provide a holistic view which means that some connections between incidents may be missed.

5.6. Attack Tree and Defence Tree

To understand an attack in terms of the attacker goals, there are other techniques used such as attack trees. Attack trees are a graphical notation where the tree root represents an attacker main goal and then it is decomposed into sub goals that are represented by the nodes [30]. These trees are useful to understand vulnerabilities; however, they do not provide details regarding the countermeasures.

To address this situation there is an extension to attack trees that includes countermeasures, these extended trees are called defence trees [31]. Defence trees present the defence nodes only on the leaves allowing a limited insight about the interaction performed during an attack. To complement this, another extension to attack trees was proposed on [32] the attack-defence tree (ADTree). The ADTrees provide an intuitive representation of interaction between an attacker and a defender of a system. These trees can then be used to support systemic corrective actions by further understanding the incident in terms of motivations. These trees may also be used to improve the organisational knowledge regarding its risks factors (e.g. impacts, threats and vulnerabilities).

Despite their capabilities, ADTrees alone do not provide a holistic view of an organisation and therefore the implications (e.g., which where the affected assets) of an attack/ IS incident may not be clear from looking at the ADTree.

5.7. Enterprise Architecture

As seen previously both attack vectors and ADTrees have some limitations in terms of being able to have a holistic view and regarding accidental incidents to address that Enterprise Architecture (EA) may be used.

EA is the logical organisation between business processes and IT infrastructure. EA benefits an organisation in five main areas, IT costs, IT responsiveness, risk management, managerial satisfaction, and strategic business outcomes [33]. In the context of this research, the main focus is IT responsiveness to IS incidents and risk management that is indirectly affected. IS incidents may be considered as part of IT responsiveness since some of them are unexpected technical problems.

With EA it is possible to produce architecture views according to the stakeholder's concerns [34]. To produce views a set of conventions for construction, interpretation and use of the architecture should be used [34]. These views improve the systemic corrective actions support since they are able provide a holistic view. The holistic view helps to understand the connections between elements related to a concern [34] which is also be useful to communicate the lessons learnt for example between ISIM and ISRM teams.

There is research performed that aimed to connect risk management and enterprise architecture [35] [36]. EA supports the creation of a roadmap for more efficient and cost-effective usage of information technology it also provides a common language for discussing risk management issues related to missions, business processes, and performance goals [37]. By combining enterprise architecture and risk driven security management it is possible to do a systemic elicitation and analysis of IS in an organisation. EA also helps to reduce the complexity of security management by modelling the relevant artefacts with an enterprise architecture [36].

In the context of this research EA is useful to enable the organisation to understand which were the assets affected by incidents, the root causes, better understand what will be affected by a given systemic corrective action, and what are the known risks for a given asset as well as to support ISIM and ISRM to communicate more efficiently.

5.7.1. ArchiMate 3.0

ArchiMate is a modelling language with a set of iconography used to address concerns related with EA [38]. In Figure 6, Figure 7, Figure 8 and Figure 9, it is possible to see some of the concepts that compose ArchiMate as well as how these concepts are related. Furthermore, in Appendix B there is a description of what is the meaning of each ArchiMate element.

Note that in Figure 6 “Active Structure Element” are the subjects that can perform behaviour. These can be subdivided into internal active structure elements; i.e., the business actors, application components, nodes, etc., that realize this behaviour, and external active structure elements; i.e., the interfaces that expose this behaviour to the environment [38].

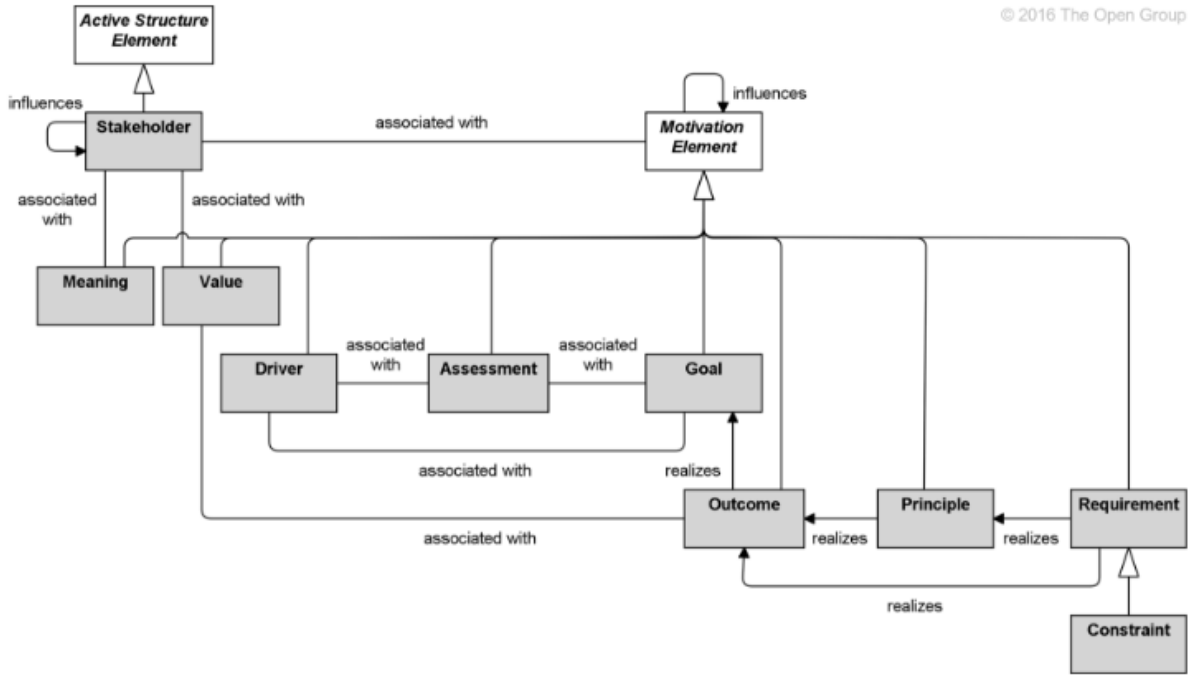


Figure 6 - ArchiMate motivation elements meta model [38].

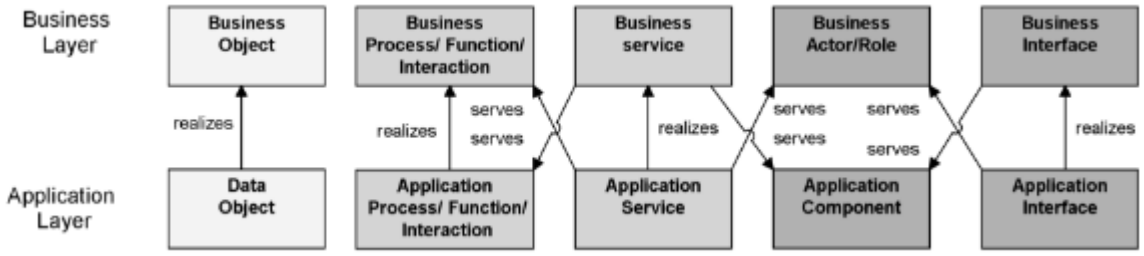


Figure 7 - Relationship between Business Layer and application Layer elements [38].

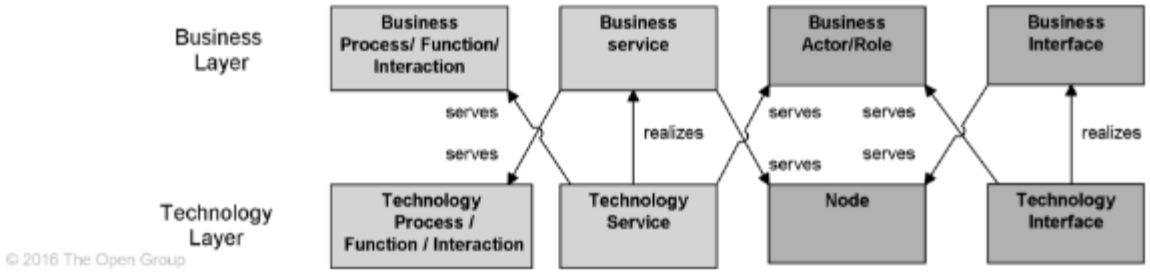


Figure 8 - Relationship between Business Layer and technology Layer elements [38].

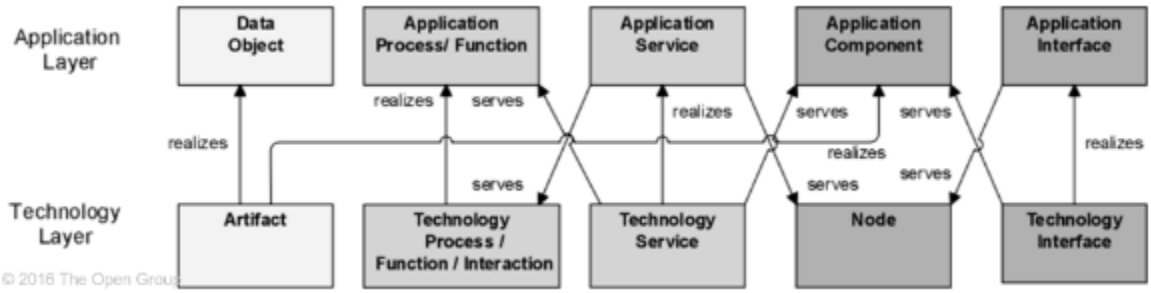
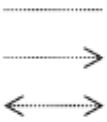
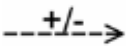


Figure 9 - Relationships between Application Layer and Technology layer elements [38].

ArchiMate 3.0 Relationships

In ArchiMate there are rules regarding which relationships can be used between elements which are defined in ArchiMate metamodels as can be seen in Figure 6 for example. In Table 1 it is possible to see the connections that may be used in ArchiMate as well as their graphical notations.

Table 1 - ArchiMate 3 relationships from [38]**.**

Structural Relationships		**Notation**
Composition	Indicates that an element consists of one or more other elements.	
Aggregation	Indicates that an element groups a number of other elements.	
Assignment	Expresses the allocation of responsibility, performance of behavior, or execution.	
Realization	Indicates that an entity plays a critical role in the creation, achievement, sustenance, or operation of a more abstract entity.	
Dependency Relationships		**Notation**
Serving	Models that an element provides its functionality to another element.	
Access	Models the ability of behavior and active structure elements to observe or act upon passive structure elements.	
Influence	Models that an element affects the implementation or achievement of some motivation element.	
Dynamic Relationships		**Notation**
Triggering	Describes a temporal or causal relationship between elements.	
Flow	Transfer from one element to another.	
Other Relationships		**Notation**
Specialization	Indicates that an element is a particular kind of another element.	
Association	Models an unspecified relationship, or one that is not represented by another ArchiMate relationship.	
Junction	Used to connect relationships of the same type.	

ArchiMate useful mechanisms

ArchiMate allows element customization to support elements beyond the ones defined in its core [38]. One of the mechanisms to customize elements is specialization. Specialization allows an element to inherit parent's properties and the relations of the general element and to change the graphical notation preferably with resemblance to the original element.

ArchiMate allows also relationship specialization which can be useful when modelling a narrow context such as ISIM by allowing the definition of more meaningful relationships between elements instead of the generic ones. Similar to element customization a specialized relationship inherits its parent properties and may have additional restrictions [38].

Another supported mechanism is relationship derivation. Derivation consists in representing indirect relationships between elements using rules such as the strength of the relationship. In ArchiMate relations have a relative strength between them. Using this relationship strength, the following rule may be applied:

"If two structural or dependency relationships r:R and s:S are permitted between elements a, b, and c such that r(a,b) and s(b,c), then a structural relationship t:T is also permitted, with t(a,c) and type T being the weakest of R and S." [38]

In practice, this can be used in this research to omit some elements from a view to be able to analyse incident patterns for example and keeping valid views according to the modelling language used.

Note that it is recommend using an ArchiMate modelling tool such as Archi to ensure that the relationships and derivation rules are correctly used.

ArchiMate advantages

In the context of this research, there is an ArchiMate extension for mapping enterprise risk and security concepts that is useful. The extension models: vulnerabilities, threat events, loss events, risks, control objectives, control measures, security principles, and other security related information as shown in Figure 10 and detailed in Table 2, note that some of the concepts in Figure 10 are not present in Table 2 since they are not the focus of this research.

By using this idea as a starting point and by proposing missing elements to the meta model it is expected that it can be used with ISIM to plan systemic corrective actions and improve the value obtained from ISIM's lessons learnt phase.

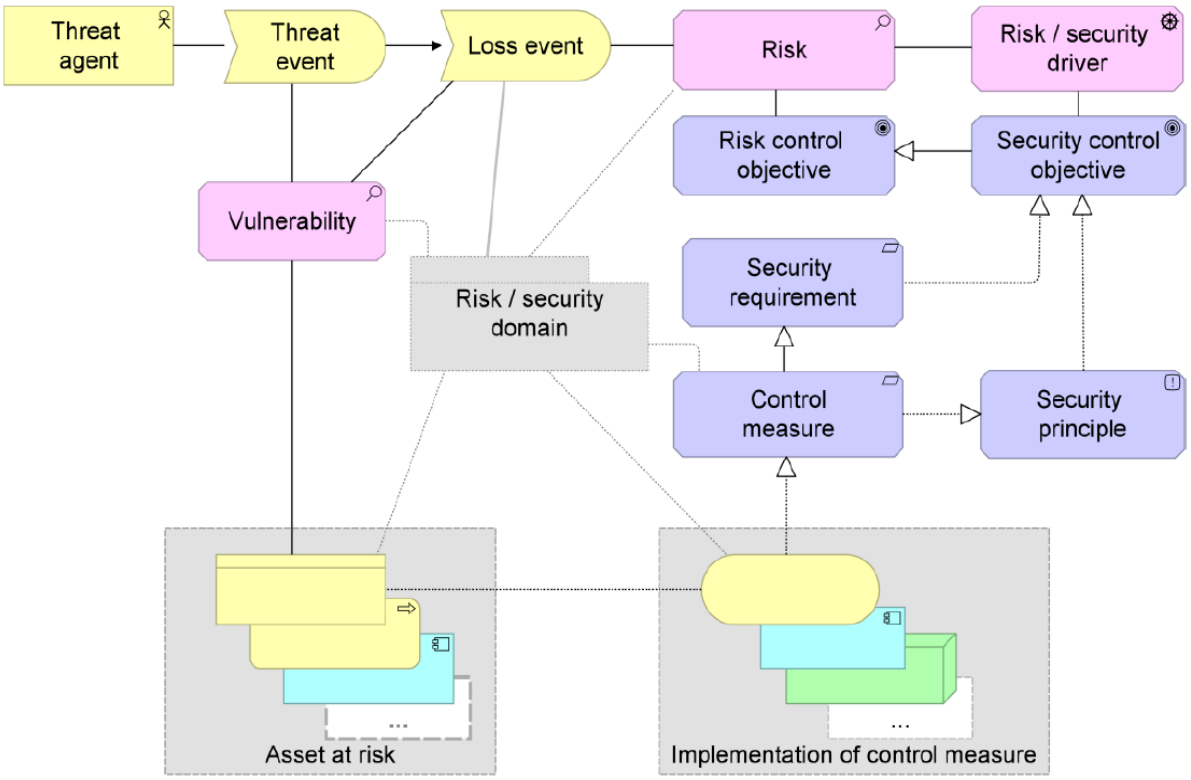


Figure 10 - Mapping of Enterprise Risk and Security concepts to the ArchiMate Language [35] **.**

Table 2 - ArchiMate Security Extension Concepts (adapted from [35]**).**

Concept	Description
Threat agent	Different types of threat agent can be modelled as different kinds of active structure elements in the ArchiMate language; e.g., a business actor, business role, application component, node, system software, or device.
Threat event	A threat event may map most naturally to a business event in the ArchiMate language. Because the concept of threat event plays an important role in risk management, it is advisable to introduce it as a specialization of a business event.
Vulnerability	A vulnerability is the result of analysing the weaknesses of elements in the architecture considering all the environmental factors that could affect the system. An example of a vulnerability is a non-encrypted communication channel over the public Internet, which means that confidential messages may be intercepted. For explicitly modelling a vulnerability, it most naturally maps to an assessment in the ArchiMate language.
Loss Event	A loss event can be mapped to the business event concept in ArchiMate, which may be triggered by a threat event. It may be useful to define a specific specialization of a business event to denote a loss event.
Domain	The ArchiMate language does not yet define a general domain concept. The location concept represents a specific kind of domain (i.e., a geographic domain). The grouping relation can also be used to group elements that belong to a certain domain, but has some limitations (e.g., it is not possible to link a group to other elements with a relation).
Risk	A risk is a quantification of a threat, and as such it maps most naturally to an assessment in the ArchiMate language. Because of the central role of this concept in Enterprise Risk Management (ERM), the proposal is to define the risk concept as a specialization of an assessment.
Control Measure	Depending on the kind of control, almost any core concept or combination of core concepts can be used to model the implementation of the control. A control may also be realized by a grouping of a number of core concepts, which is something that cannot properly be modelled in the ArchiMate language.

5.7.2. Enterprise Architecture Management System

Enterprise Architecture Management System (EAMS)[2] is a software tool used for EA. It eases the burden of keeping architectural representations up-to date since it generates views, which are called blueprints in EAMS, automatically using the rules defined by the user.

EAMS functionalities

EAMS also allows Meta-model definition, which means that it is possible to define the relations between the concepts. Defining the meta-model gives flexibility to adjust the tool to the needs. In the context of this research it presents an advantage since the extension of existing meta-models, such as ArchiMate meta-model, is necessary.

EAMS has mechanisms that allow data importation from other sources such as spreadsheets or relational databases, this means that information can be uploaded in batches reducing the effort in situation that the information to be used is already available in another format. However, some changes may be needed since the defined meta-model may be different from the dataset that will be imported. It also takes some effort regarding data quality since if for example database normalization rules are not respected, EAMS will not normalize data automatically, despite having mechanism that simply merging instances.

Blueprints are defined using the interface shown in Figure 11, note that the image is cut for visualization purposes. This interface allows the definition of the composing cells as well as the queries that will feed them. It is also here that the visual aspects are defined. In Figure 12, it is possible to see the resulting blueprint. Queries are defined using ERML which is an XML-based language with a logic like SQL. The syntax of this language is available in EAMS manual; however, this language is not widely used.

EAMS has also a life cycle functionality allow the visualization of which elements are active or inactive in a given time interval using highlights in the elements of the blueprint.

[2] http://www.linkconsulting.com/eams/, accessed on 11/12/2016

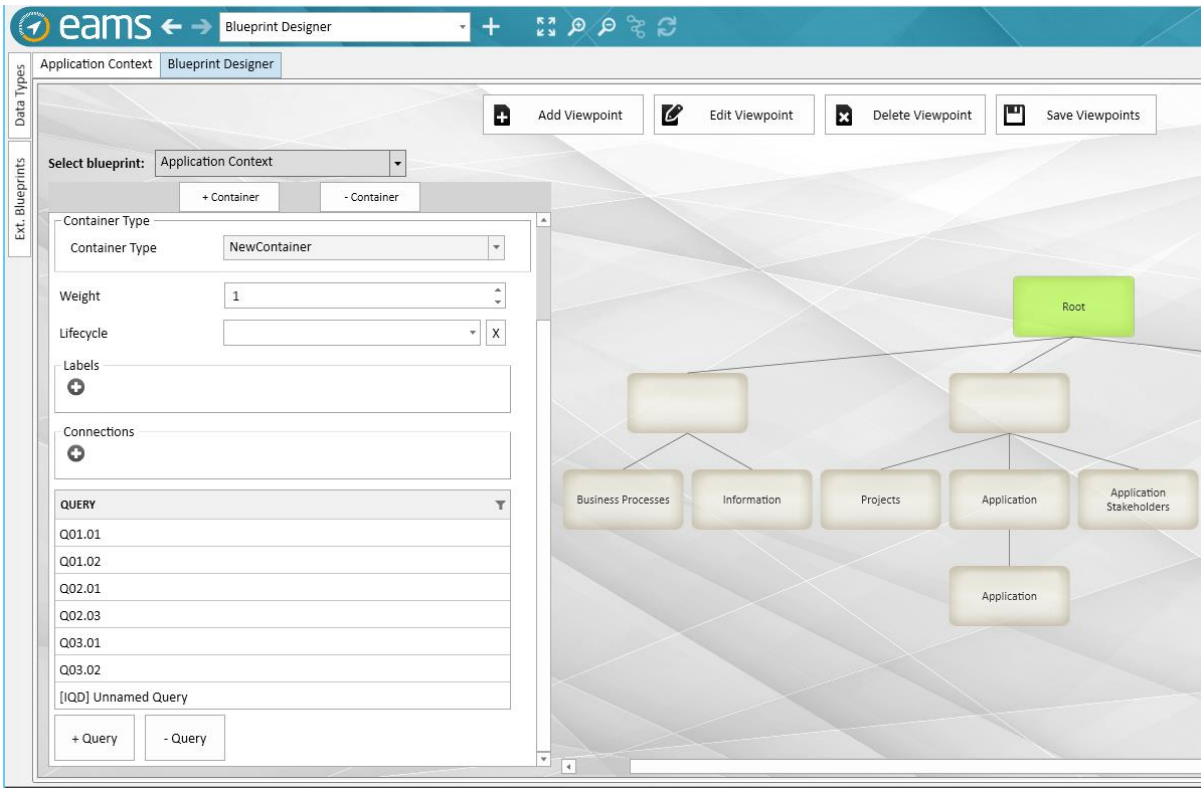


Figure 11 - Blueprint designer interface

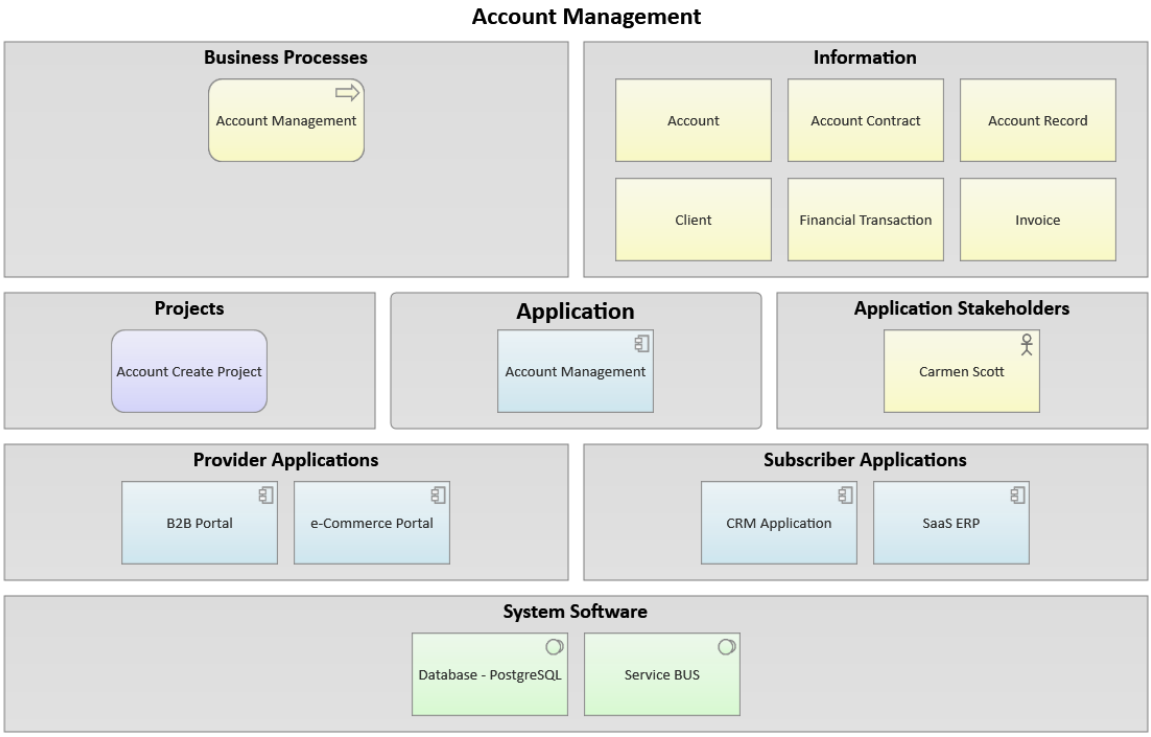


Figure 12 - Resulting blueprint

EAMS advantages

This tool is valuable to understand which elements are connected in complex architectures since it enables the user to see relationships in views based on rules defined using queries, this automatically generated visual element gives EA flexibility to the views which makes EA easier for humans to interpret complex scenarios.

In the context of this research it will be valuable to analyse the architecture from different perspectives (e.g., events, risks, vulnerabilities, assets or combinations between them) as so a tool such as EAMS, that allows the creation of views with less effort than when just using a modelling tool such as ArchiMate, is beneficial.

5.8. Summary

Through the literature analysis it was observed that organisations do not perform systemic corrective actions and the lack of communication between ISIM and ISRM teams [7] [16]. However, the need for these actions was identified [7] and its long term benefits [23].

With the objective of identifying techniques and tools to support systemic corrective actions regarding ISIM it was found that modelling languages such as ArchiMate and tools such as EAMS could be used. There were also other techniques identified such as ADTrees and representations of attack vectors.

Theories such as double-loop learning and the DSL were also identified with the objective of improving what is already described in ISO and NIST standards regarding incident management learning phase.

In Table 3 it is possible to see a comparison between attack vectors representations, ADTrees and EA views, to understand which one presents better capabilities to support ISIM learning phase and systemic corrective actions.

Identifying patterns is an important step to be able to learn from incidents, as so this is one relevant criteria when analysing the potential that these technics may bring to this research. Attack vectors representations are used to represent the flow of one attack as so when the objective is to have a high-level view on how incidents may be related they are difficult to use. ADTrees are focused in the goals of an attacker which may be used to summarize the goals of occurred IS incidents but as happens in attack vector representations, it is difficult to view the multiple IS incidents simultaneously using ADTrees in a way that helps to identify patterns between the IS incidents.

ADTree has higher values than attack vectors representations for systemic corrective actions implementation support since it allows to act based on the attacker goals which provides a wider view

than attack vectors representations, making easier to understand how a corrective action will affect the system instead of how it will affect in that particular attack. We consider EA support to be higher since by having the IS incidents associated with business assets it provides both a high-level view of the incidents and the exact assets that were affected.

In terms of communication it ADTrees are also better than attack vector representations since it is easier to explain the attacker goals than the details of the path that the attacker used. EA is considered to be better since it allows a holistic view. A holistic view improves the capability to understand the connections that are relevant for a given IS incident and the ease of communication between parties like ISIM and ISRM but also inside of ISIM for example for the activities mentioned in DSL.

Despite the existing related work, literature lacks a methodology to support systemic corrective actions in ISIM by providing a holistic view. Therefore, such methodology will provide a new approach toward ISIM and will potentially bring benefits towards the existing approaches.

Table 3 - Summary of the capabilities of the analysed techniques.

	Support to identify IS incidents patterns	Support for systemic corrective actions implementation	Support for communication between different teams	Holistic View
Attack Vector representation	Low	Low	Low	No
ADTree	Low	Medium	Medium	No
EA views	High	High	High	Yes

6. Solution

As analysed in section 5.2 systemic corrective actions may be used as input for double-loop learning, which provides long term benefits for the organisation where it is applied. Moreover, in sections 4.2.4 and 4.3, it is explained the importance of having effective communication between ISIM and ISRM. It was also observed in section 5.7 that EA is able to provide a holistic view and that there are already proposals on how to use EA for risk management.

6.1. Objectives

The main objective of the solution is to use EA to support systemic corrective actions in ISIM. The research aims also to:

- Improve learning capabilities in organisations.
- Use a common language (i.e., EA) in ISIM and ISRM within the organisation to support for ISRM teams to use as input the knowledge produced along the ISIM, particularly in the lessons learnt phase.
- Find an appropriate tool to support systemic corrective actions in ISIM.

By using EA and ArchiMate modelling language with the previously mentioned extension for risk and security shown in Figure 10, it is possible to ease systemic corrective actions by for example modelling the new vulnerabilities as incidents occur and as they are further analysed.

In the beginning, benefits from using EA tools such as Archi or EAMS may not be evident, however as complexity increases in terms of vulnerabilities, threats, risks, and other security elements, the larger the benefits will be. This is expected to happen due to the fact that as the architecture is updated with more information, the easier will be the root cause analysis as well as the relation between incidents and assets due to the clarification of the relations between the assets, vulnerabilities, threats, risks, and incidents. This relation can be used to react to the incidents and also to learn from them after the responses phase.

Modelling EA with the purpose of improving ISIM, will also potentially improve ISRM. However, for this to be possible, IS incidents and IS risks need to be registered with attributes that are comparable (e.g., IS incident impact and IS risk consequence value should have the same numeric scale and comparable criteria for its attribution). To improve ISRM using ISIM it is also necessary to have a database with explicit association among incidents, risks, controls and assets. Risk is attributed to assets and incidents affect assets. By understanding which assets were affected by an incident and which were the risks that had materialised into incidents may be possible to identify other potential risks and treat them.

This association may be able to contribute to risk analysis in terms of probability and consequence as incidents are solved and analysed in lessons learned phase. The planning phase of ISIM may also benefit due to a faster translation of risk into the related incidents, however this is out of the scope of this research since it is more related with risk management's monitoring and review, not ISIM.

In Figure 13, the possible relationships between ISIM and ISRM are presented with green arrows and the black arrows represent the flow inside of each of the mentioned processes, ISIM and ISRM. These relationships may be between ISIM's "detection and report" and ISRM's "Risk Monitoring and Review" that is supported by [3] [19], ISIM's "Lessons Learnt" and ISRM's "Risk Monitoring and Review" supported by [7] [23], and between ISRM's "Risk Monitoring and Review" and ISIM "Plan and Prepare" supported by [19].

These connections represent one of the opportunities that double-loop learning provides in the context of ISIM in the sense that besides using ISIM for reducing incidents impact it can be also used to change the organisation's mental model regarding IS incidents and risks. This means that by using double-loop learning, it is possible to improve risk management. In the context of the proposed methodology, the connection between "Lessons Learnt" and "Risk Monitoring and Review" is the most relevant since it is the one that uses the knowledge acquired in the Systemic Corrective Actions phase and is used to propagate it in the "Perform Double-loop Learn" phase. Note that in Figure 13 this connection is highlighted in red.

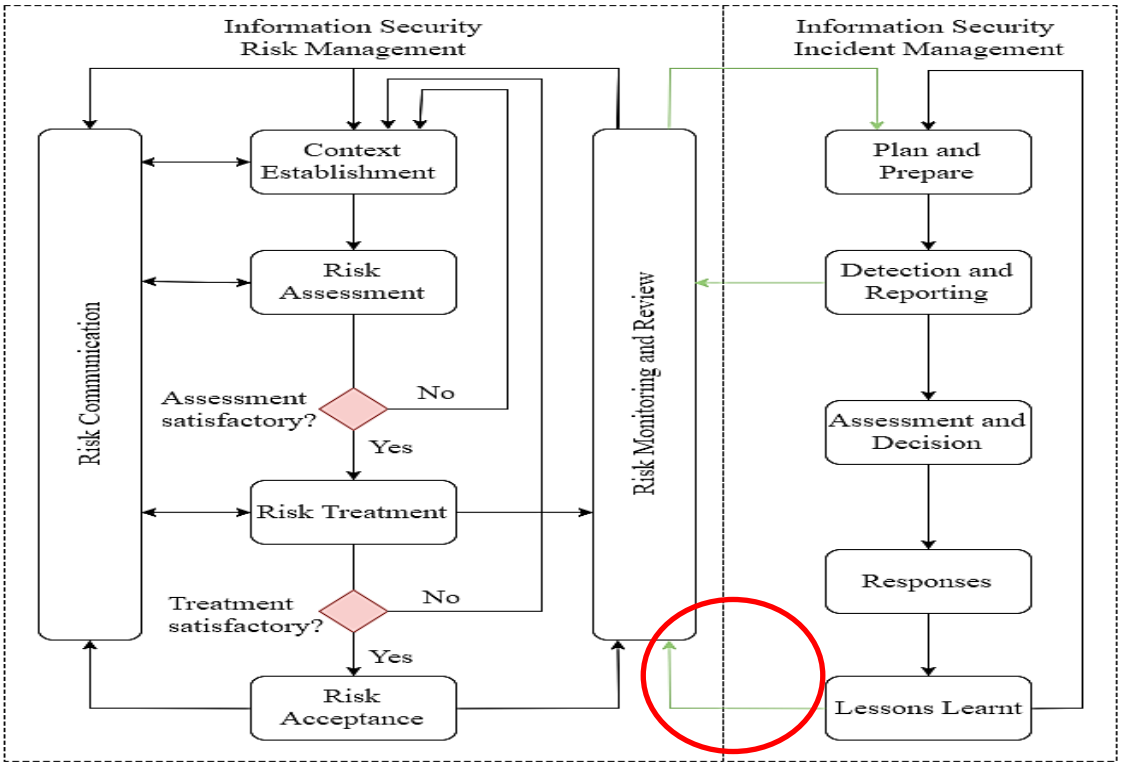


Figure 13 - Connection between ISRM and ISIM (modified from [19] [26]**).**

6.2. Metamodel to support ISIM

To address the research objective that refers to the use of a common language to improve communication and represent IS incidents and other IS security related concepts in ArchiMate, we decided to use Figure 10 [35] as the base metamodel and to adapt it from the context of this research.

We decided to specialize business event concept as can be seen in Table 4. The IS incidents were represented as ArchiMate's business events since they are events that potentially affected the business, however they were represented in red to highlight the negative impact associated with it. These incidents have an impact value associated with them for each of the CIA properties and a relation with one or more risks that may or not exist in the organisation's IS risk database.

Table 4 - IS Incident specialization

Parent Concept	Specialized Concept	Description	Graphical notation
Business Event	IS Incident	Event with negative impact towards an asset.	

In Figure 14, IS incidents are connected with vulnerabilities since IS incidents need a vulnerability to happen. A threat event triggers an IS incident by exploring a vulnerability and a threat event to explore the vulnerability. IS incidents may affect one more assets or groups of assets, consequently they are associated in the metamodel. IS incidents may happen due to a problem in a control measure which is expressed with the association connection. IS risks and incidents are closely connected and similar in the sense that one represents a potential loss and other an effective loss that occurred and therefore they are also associated.

Some of the relationships in Figure 14 were kept unchanged from Figure 10, an existing mapping of enterprise risk and security concepts in ArchiMate, and some result from deriving the relationships in that same figure. These ArchiMate techniques are briefly described in section 5.7.1.

Note that the proposed methodology gives flexibility regarding which assets should be represented and that was considered in the metamodel as can be seen in Figure 14 by using ellipsis for the assets in the grey rectangles. The proposed metamodel can be used by organisations concerned with ISIM and ISRM to help communicate about relevant IS elements and their contexts.

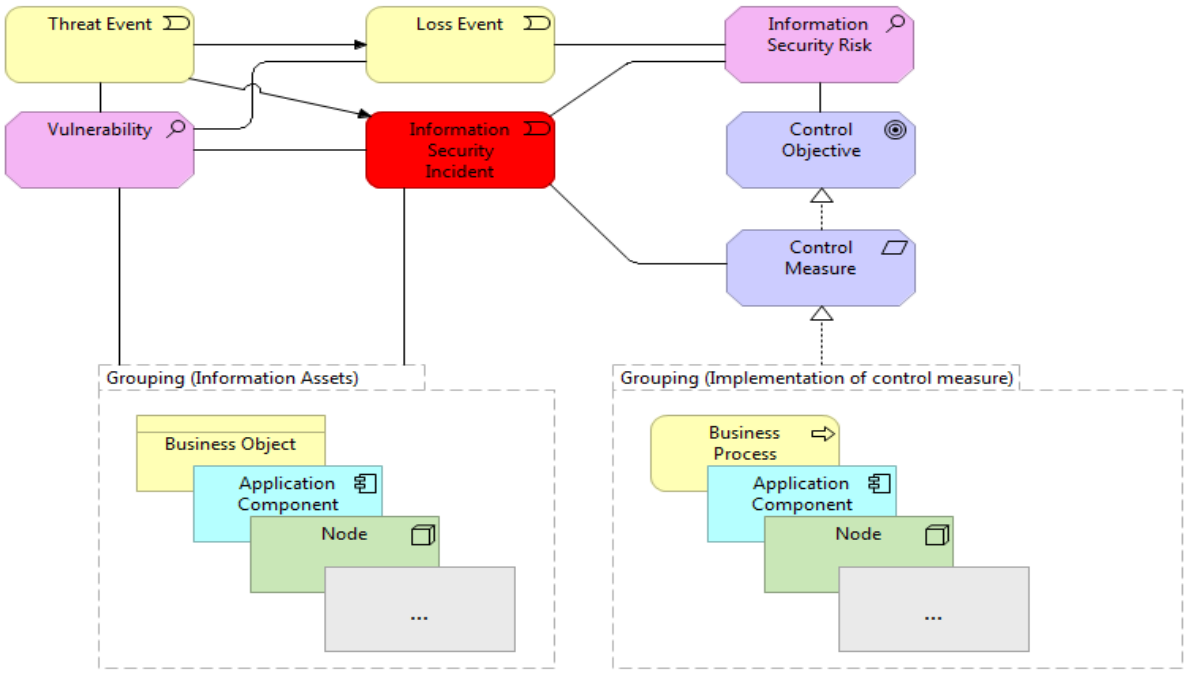


Figure 14 - Information Security Management proposed meta-model

6.3. Methodology

Considering the research objectives, we propose **a methodology supported by EA to support systemic corrective actions and double-loop learning in ISIM, as illustrated in Figure 15.**

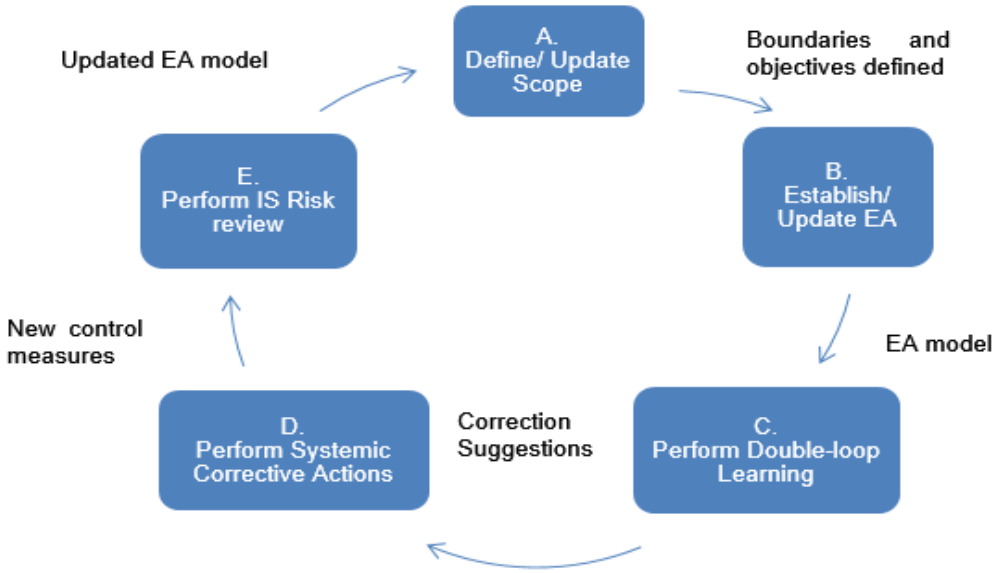


Figure 15 - Methodology to support ISIM's lessons learnt phase and systemic corrective actions using EA.

Figure 15 presents a methodology to support systemic corrective actions and double-loop learning that is supported by EA. This methodology is temporally located alongside ISIM's lessons learnt phase (phase A, B, C and D of the proposed methodology) and ISRM's monitoring and review phase (phase E of the proposed methodology). Figure 13 helps to clarify the flow mentioned between ISIM and ISRM. Note that using EA during the whole ISRM process is recommended to ensure that the EA is updated and that the teams are familiar with the concepts to allow an effective communication. It is also recommended the use of a modelling language such as ArchiMate. Tools such as EAMS can also be used along all the methodology to ease the effort to maintain EA updated and to provide different blueprints of the EA making it easy to be understood by the participants and without much effort in their production.

The phases presented in Figure 15 are further detailed in the following sub sections. Business Process Modelling Notation (BPMN), a graphical notation for business processes, was used to highlight the steps that should be performed in each phase. Note that the roles used represent the role that should be accountable for the associated steps, it does not mean that in practice the step cannot be performed by another role such as one that is hierarchically below the role suggested in BPMN.

6.3.1. Phase A - Define/Update scope

Understand the limits on which the ISIM is relevant and identify the assets that have known IS risks. It should be defined by security management and senior management.

In Figure 16 it is possible to see the steps that should compose this phase to achieve an EA that is adequate for the organisation following the methodology. To ensure these results it is fundamental to ensure that the organisation's purpose, context, and security objectives are defined and known by the person that will model it, the enterprise architect.

The scope may be updated between iterations in the methodology resulting from the newly identified IS risks or assets for example. In some cases, the best approach would be to include the entire organisation, however the costs associated with such decision could be too high and therefore it is recommended to start by including only the information assets used for core processes instead of every asset a company owns and with time adjust the scope as IS incidents occur or new risks are identified.

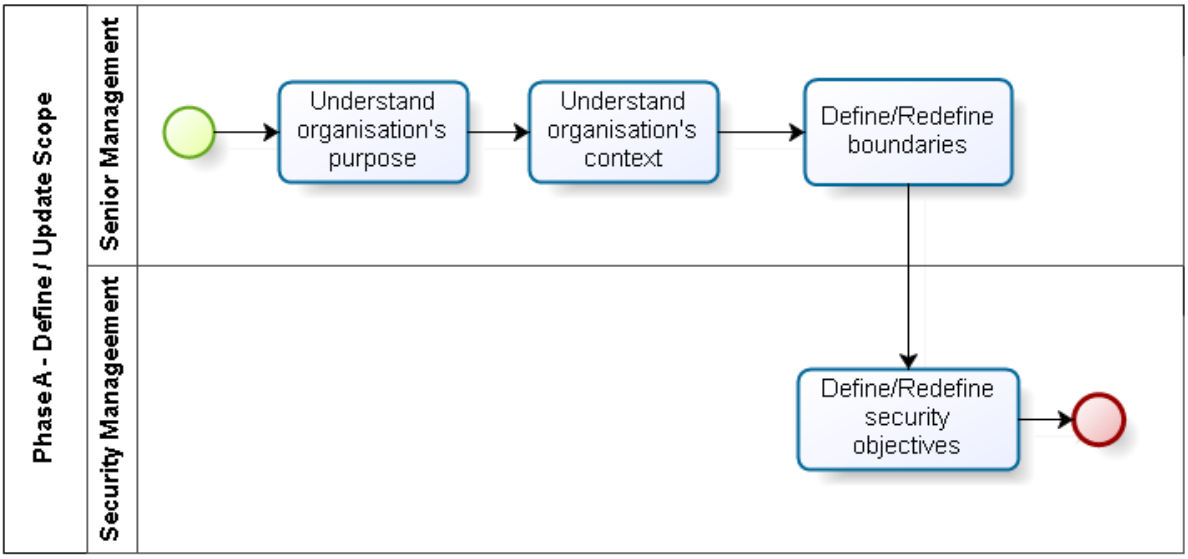


Figure 16 - Phase A process

6.3.2. Phase B - Establish/Update EA

Using the defined scope, in the first iteration the EA is developed and in following iterations the EA is updated if necessary. The EA should contain elements related with IS risks, IS incidents as well as the core elements related to business, information systems, and technology. EA should be defined incrementally according to the needs (i.e., some assets with homogeneous characteristics may be grouped to ease this phase and then these groups may be further detailed or abstracted if it presents advantages regarding the understanding of IS incidents and IS risks for example). The granularity in terms of asset's details should be adjusted over iterations to ensure that the model is useful.

In Figure 17 it is possible to see the steps that compose this phase. This phase starts by adjusting the metamodel which means that the modelling level that will be used should be defined (e.g., should the relationships between application components be abstract or should the Application Program Interface (API) used be identified), to have homogeneous data across the organisation. After that the assets should be identified. With a list of assets, the following step should be to identify the relations among assets. After that IS risks should be related to the assets, by knowing the existing assets in the system and how they are connected this step will be easier. Furthermore, the existing control measures should also be identified and related with the IS risks. To conclude this phase, IS incidents should be associated with the previously mentioned elements, assets, IS risks, and control measures.

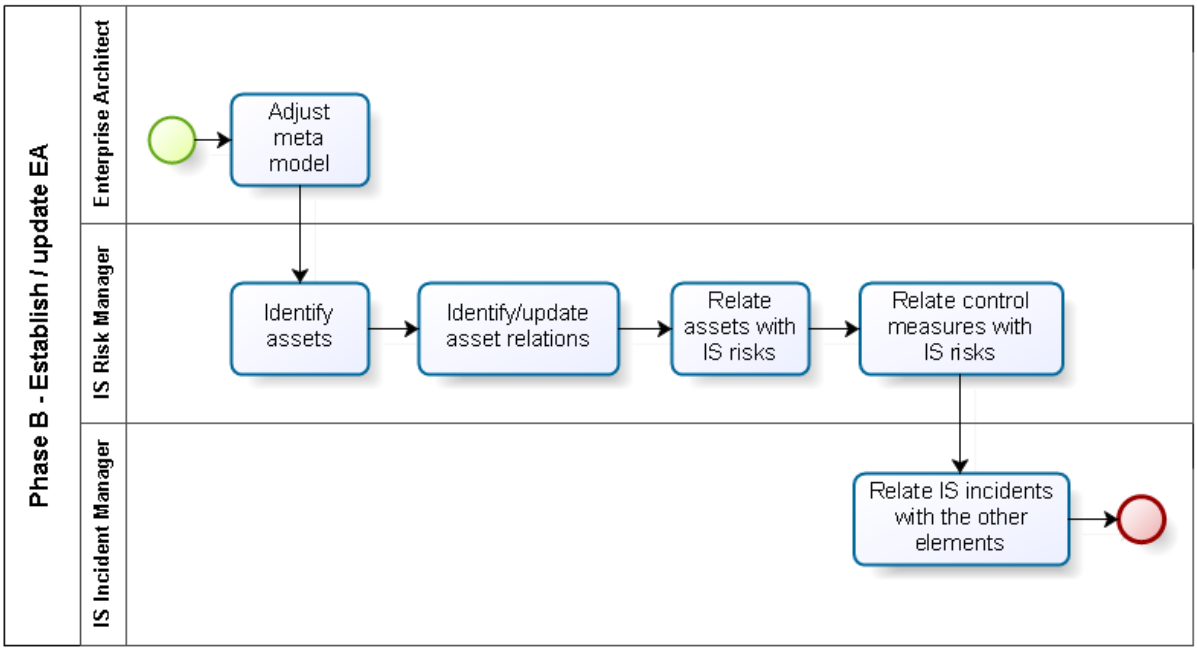


Figure 17 - Phase B process

6.3.3. Phase C - Perform Double-loop Learning

Understand how the control measures used to respond to incidents can be generalised to be applicable to other vulnerabilities of the company and disseminate the knowledge obtained with the incident (e.g. incident impact, new risks, controls implemented) with the relevant stakeholders particularly with the security management, and senior management (as described in Figure 5) but also ISRM team in order to enable them to be aware of what have changed and how it is expected to reduce the impact or likelihood of some risks. To this purpose, EA can once again be used to ease the communication. EA may help to identify incident patterns and consequently help to identify the best control measures. These patterns include but are not limited to temporal relations (e.g., incidents that usually occur at a particular hour in the day), geographical relation (e.g., incidents that usually occur in a particular room), resource relation (e.g., incidents that usually affect the same machines), and chain relation (e.g. sequence of incidents that usually occur together). Then according to the identified issue solutions should be identified and proposed with supporting EA TO-BE models.

In Figure 18 the steps that should be performed to be able to learn effectively from incidents are presented as well as the propose of the roles that should be accountable for each step.

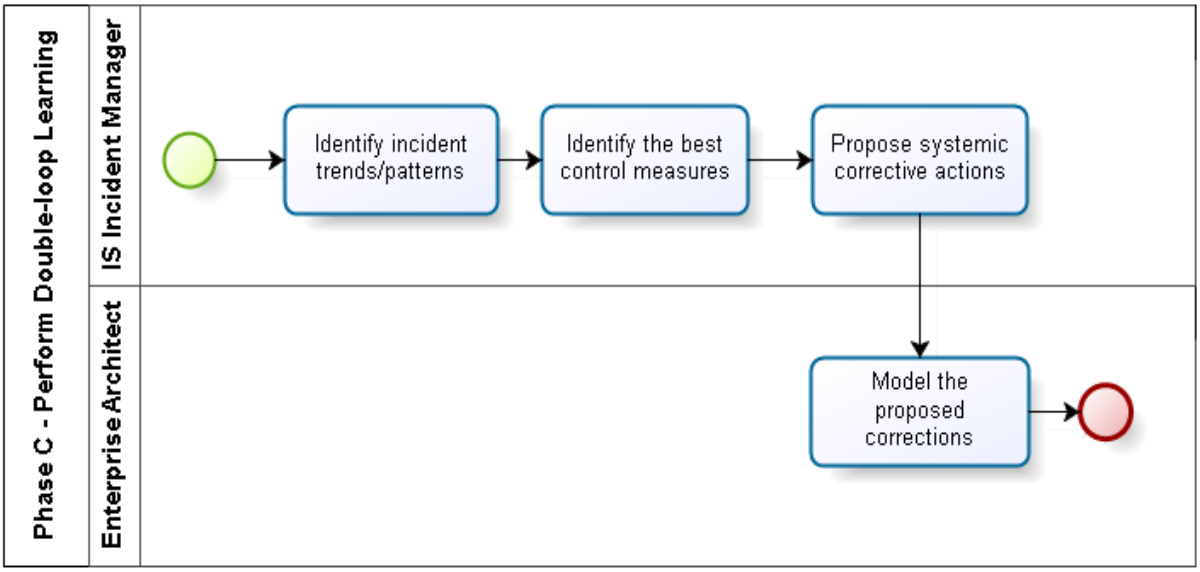


Figure 18 - Phase C process

6.3.4. Phase D - Perform Systemic Corrective Actions

Use EA and the knowledge from phase C to enable the evaluation of possible solutions to address the root cause found. Examples of these solutions are the change of policies, change of processes, and change in the technology and applications used.

As shown in Figure 19, in this phase the senior management should evaluate the proposed corrections, including the EA models, and decide and justify which are the best options for the organisation. Note that the best option in a given moment may be for example, to delay the change due to budget constraints or resources availability. Then if the decision is to implement a control measure, the security manager should ensure that everything is performed as planned. With the controls implemented the EA should be updated accordingly and then the security manager should promote a risk assessment.

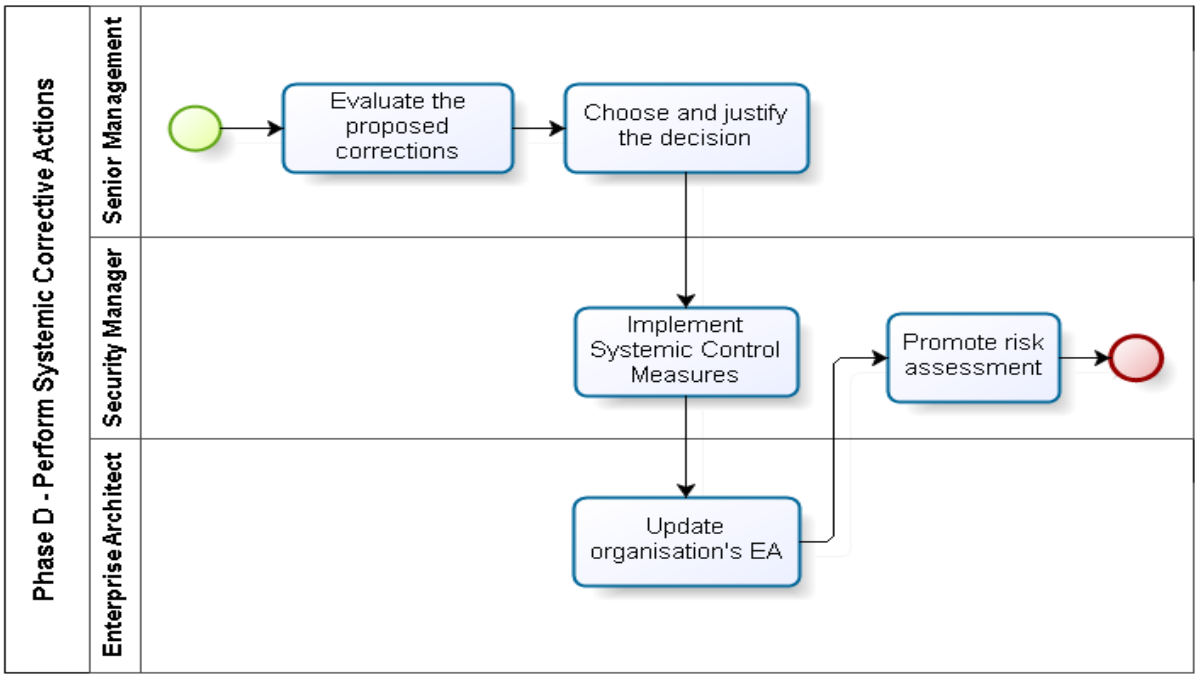


Figure 19 - Phase D process

6.3.5. Phase E - Perform IS Risk Review

According to what was learned in phase C and based on the systemic corrective actions performed in phase D, the ISRM team should identify and analyze new IS risks, and re-evaluate the previously identified ones. EA supports this phase by providing a simple way to expose which IS incidents were related to this incident as well as which controls were implemented since the last evaluation. Considering this information, it is possible to evaluate IS risks supported by a holistic view of the system and the relevant factors that contribute for it.

In Figure 20 it is possible to see the steps that compose this phase in order to make use of the EA effectively. Note that despite not being represented in the process IS Risk Manager may also propose new controls or adjustments in the existing ones that would then need to be evaluated and approved by senior management if they correspond to major changes (Phase D).

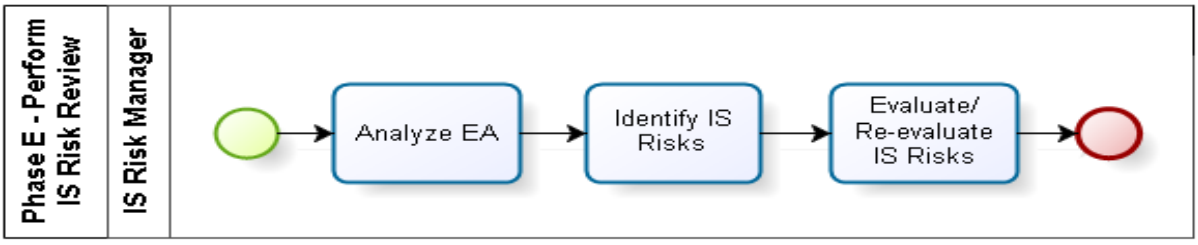


Figure 20 - Phase E process

6.3.6. Observations

The proposed methodology presents a guideline and does not force someone using it to perform every step in each iteration. The phase A, for example, may be skipped in the second iteration if there are no internal and external changes like different suppliers or new competitors. The iterations should also be performed with different periodicity in different organisations depending on their size, available resources, sector, and other factors. However, we propose to perform at least one iteration per year, since it will probably ensure enough data to extract some conclusions from it even in smaller organisations.

Note also that the organisation does not need to have a full-time enterprise architect as long as the changes and the incidents are registered and the communication with the domain experts is possible whenever clarifications are required. However, in the first iteration its work is particularly important since it is mandatory for everyone involved to understand EA, otherwise the methodology will provide lower benefits.

6.4. Supporting Tool

To be able to perform this methodology more efficiently it is recommended to use a tool that can be used along all the methodology. Using EAMS it is easier to identify the relations with assets than with ArchiMate in complex scenarios. When compared with spreadsheets EAMS avoids errors in the data provided or lack of data due to the difficulty in finding or understanding what is required by the ones responsible for IS incident reporting within the organisation.

EAMS also works in cooperation with tools that are already used by organisations such as spreadsheets for registering assets, IS risks and IS incidents in the sense that what currently exists in these spreadsheets can be imported to EAMS using its embedded data integration mechanisms and the data added in EAMS may also be exported to a spreadsheet.

The blueprints presented only require effort in its definition, once the relevant elements and connections are defined, it is only necessary to add more instances and the connections between them, meaning this that the visual part is automatically generated. EAMS also allows to navigate through blueprints provides a faster way to analyse the information that an organisation possesses regarding their assets, incidents and risks.

Considering this, we configured EAMS to support this methodology. This configuration consists in defining the metamodel has can be seen in Appendix C, importing the data into EAMS (data instances), defining the relations between instances, and defining appropriate views for the stored data (blueprints) using a query language.

6.5. Summary

By extending ArchiMate's metamodel to include IS incidents, defining a methodology to support systemic corrective actions, identifying and configuring a tool to support the methodology, we present solutions aligned with the research objectives identified in section 6.1. Together, and with the necessary expertise, these elements provide a new approach to ISIM and IS in general that uses IS incidents to reflect on how the organisation operates and to improve its processes.

7. Demonstration

The demonstration is used to make evident the use of the artefact to solve one or more instances of the problem [10].

The proposed methodology was tested using DemoCorp data. DemoCorp has its information security management system ISO 27001:2013 certified. However, according to its responsible, its learning phase was ineffective. The demonstration was performed using DemoCorp's data with abstractions due to confidentiality constraints.

7.1. Simulation

Making use of DSRM iterations, before being used with DemoCorp's data, the proposed methodology was simulated using fictional data to clarify and tune its phases, as present in this section.

Supposing DemoCorp has a card production process. In this process, there are two assets: card production support information (e.g., serial number, card template, logs) and client's information. These assets are available through an Enterprise Resource Planning (ERP) software (e.g., SAP).

Supposing now that the risk of unauthorized access was identified for both assets and the control for it was to use an antivirus in all personal computers of the organisation. After the risk identification, an IS incident occurs and affects card production support information related with the machine parameterization data. The incident consists in unauthorized access using computers inside the organisation.

By decomposing the incident and doing a systemic corrective action using EA to improve causal analysis and follow up to systemic corrective actions [7], it will be possible to note that the incident that affected the card production documentation may also occur in client's information. This happens because the controls are the same between these two assets therefore this vulnerability affects both.

In this situation, this incident will lead to a control with a wider scope, affecting two assets instead of one as it would occur in single-loop learning with direct corrective actions.

This simple example may seem to be obvious and not to require any supporting tool to achieve the result. However, the reality is usually more complex. This complexity comes from the fact that it is common for an organisation to consider a larger scope and consequently have more assets, risks and incidents to manage. It may lead to such a complexity that becomes humanly not feasible to be aware of all the connections without a supporting tool.

Considering this, it is presented below the application of a simplified version of the proposed methodology supported by EA modelling language, ArchiMate.

Phase A – Define scope: In this case the purpose of the organisation is to produce cards. We can suppose that the organisation is focused in the production of the card and imports the raw materials. This organisation also uses an ERP from another organisation and doesn't have any software developed by themselves. For the boundaries, we can suppose that DemoCorp has other processes which are not security sensitive. Regarding the security needs it is necessary to ensure that these cards cannot be replied.

Phase B – Establish EA: In Figure 21 part of the EA is represented according to the scope defined in phase A. The assets are card production support information and client's information. Note that this model is using the extension for ArchiMate proposed in this research.

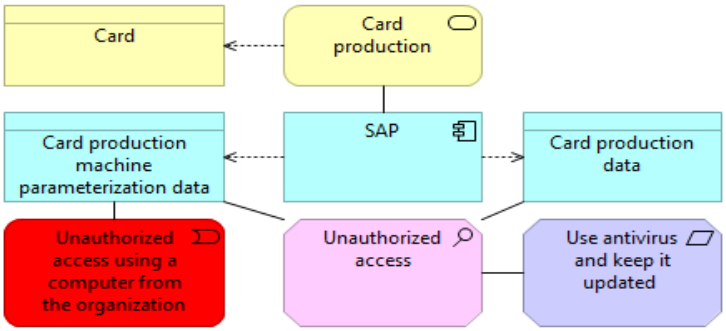


Figure 21 - Card production context using ArchiMate.

Phase C – Perform Double-loop Learning: Learn that all the information should have privileges according to least privilege principle by default. Understand that incidents related with availability of the documents may occur due to the change in privileges.

Phase D – Perform Systemic Corrective Actions: Review the access privileges, ensure least privilege (i.e., only the users that need the information, have access to it). In Figure 22 this review is represented as a control measure in ArchiMate. Note that the direct corrective action would be to block the user that is performing an unauthorized access.

Review access privileges for all the documents in the ERP and ensure that least privilege principle is being followed. Ensure that future documentation follows this principle by default. Figure 22 represents the addition of a security principle in the scope of the card production.

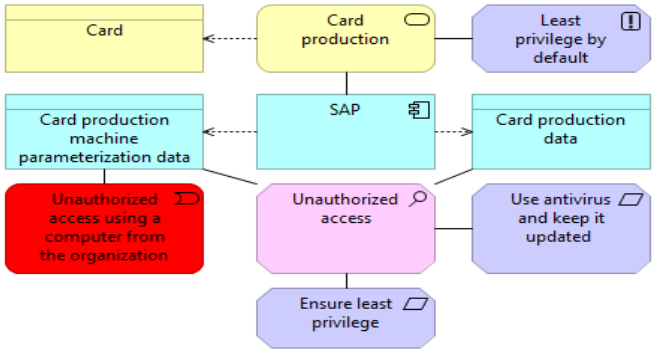


Figure 22 - Principle addition due to double-loop learn.

Phase E - Perform IS Risk Review: New risk identified, “unavailability of information due to wrong privileges attributed”. Figure 23 represents the addition of a new risk due to the new principle added in the previous phase.

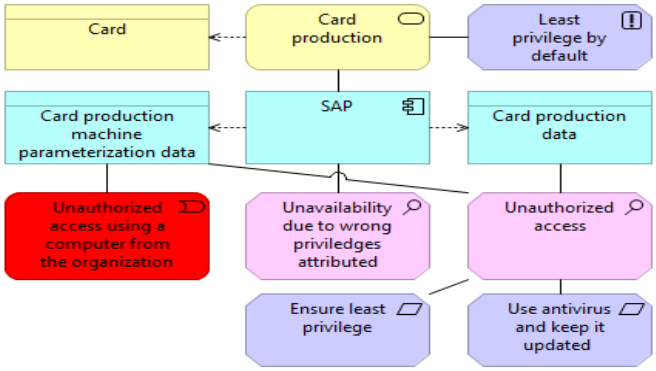


Figure 23 - New risk identified due to the addition of a principle.

Limitations

After this demonstration, when trying to use ArchiMate as represented here and the modelling tool Archi, the modelling complexity and effort increased considerably since when a new IS incident or IS risk was added, for example, it sometimes required to change the whole model in order to maintain it legible.

Considering this simulation and DSRM iterations, we decided to improve the solution by proposing the usage of an EA management tool that reduces the effort to update a model by handling the visual part of modelling an EA and ensuring data quality. To achieve this, we decided to use EAMS since it also provides the flexibility necessary to use the proposed extension to ArchiMate’s metamodel.

7.2. Field Study

The methodology proposed in section 6.3 is applied below considering the reality of DemoCorp.

7.2.1. Phase A - Define/Update Scope

DemoCorp has the scope defined since their ISO 27001:2013 certification covers only one production process, the production of one type of card. Despite this limitation in scope for some assets it is not clear for the collaborators whether they should be considered or not. This is a learning process that will expectably be refined at least once a year during the mandatory risk review imposed to maintain the certification as well as the internal and external audits.

Following the process defined for phase A and considering the limitations regarding the confidentiality associated to the organisation we have the following steps:

Step 1 - Understand organisation's purpose

DemoCorp purpose is to produce a set of physical products that have security mechanisms.

Step 2 - Understand organisation's context

Regarding the context, this company has some international competition for part of its products and no competition for other products. The security of these products is a key property and it must be ensured. Most of the products need to follow international standards to be produced and delivered and have certified processes.

Additionally, since DemoCorp already has ISRM and ISIM processes it is important to understand them as part of the internal context of this organisation. These two processes are relevant to this research since they explain how the data used in the demonstration was obtained and who were the providers and the validations that it has. In the next paragraphs of this subsection the two processes are further detailed.

DemoCorp's Information Security Risk Management AS-IS

DemoCorp currently conducts IS risk analysis in the context of ISO 27001:2013. This analysis follows three major phases: i) asset identification, ii) IS risk identification, and iii) IS risk treatment.

This process is performed and documented at least once a year and when significant changes regarding the existing assets, controls or organisation context occur (e.g., when there is a change in law that affects the organisation), additional risk analysis are performed.

i. Asset Identification

During asset identification phase, the assets related with the certified production process are identified by each department and categorized according to an existing list with categories such as human resources, hardware, software, processes, services, and information. The identified assets are classified in terms of confidentiality divided in five levels. The owner of each asset is also identified in terms of his role and the IS department monitors the process to ensure that the relevant assets are identified.

After this, the assets are grouped according to its characteristics and its owner and are valued in terms of each of their CIA properties using the same five-level scale. This evaluation is performed in order to understand how important these assets are to the organisations and force ISRM teams to reason how a failure in terms of confidentiality, integrity or availability would affect the certified production process. Considering the average of three CIA properties the ones with an average above the policies' established level, which currently is three, are a target for risk identification. This differentiation exists to optimize the resources by avoiding spending time with assets with lower value for the process.

The Chief Information Security Officer (CISO) or the IS committee may act during the process to guarantee that the relevant assets are appropriately identified, categorized, classified, and grouped in terms of IS by asking for a review or justifications for the decisions taken.

ii. IS Risk Identification

In DemoCorp, IS risk identification, is performed by the IS risk manager of each department. IS risk managers, identify the risks of their department's assets by identifying vulnerabilities and threats as well as the likelihood of a threat to exploit a vulnerability and the consequences of such event.

The know-how of each area is limited in terms of the identification of vulnerabilities and threats of their assets and controls as well as the probabilities and impacts associated with possible events. This happens due to the different specializations amongst departments.

The likelihood is identified based on the organisation's historic and has five different levels. The consequences are defined based on the sum of the consequences in each of the CIA properties that may vary between five levels. Then considering this, in DemoCorp, the risk level is calculated using the product of these two components using Equation 1. This equation has a maximum value of 75 (i.e., (5+5+5) × 5) and the risk classification used is based on this value.

Equation 1 – Risk level of Risk R

$$\boldsymbol{Risk\ level}\ (\boldsymbol{R}) = \big(\ Confidentiality(R) + Integrity(R) + Availability(R)\big) \times Likelihood(R)$$

In this phase risks are associated with the defined asset groups. Considering this, the groups need to be well defined in order to ensure that the identified risks are valid for all the elements of the group and also to ease the definition of control measures (i.e., if a control measure can be applied to one of the assets in the group it should also be applicable to the others without major modifications).

First the risk is calculated without considering the currently implemented security controls. Then the existing controls are identified and the risk level is re-evaluated having them into account. When the risk level is above a defined level it must be considered for the IS risk treatment phase.

Note that the risk identification is then centralised and analysed by the ones with greater responsibility regarding DemoCorp's information security, the CISO and the IS committee if necessary, and as so what was identified may be adjusted according to the decision.

iii. IS Risk Treatment

In this phase, the risks with a level above the maximum defined in the organisation's policies are addressed for treatment. The objectives for the controls are identified and solutions are proposed and evaluated in terms of predicted costs and benefits. Based on the cost benefit relation and the risk level the IS committee decides whether the proposed controls should be implemented. When the implementation is approved, each department needs to monitor their risks and perform a risk assessment after the implementation of the control to evaluate its effectiveness.

Later the risks are transmitted to the information security committee by the CISO and if their treatment is approved then each department needs to monitor the control implementation and perform an impact revision considering the new controls implemented to understand if further measures are necessary. If additional measures are required, the process performs a loop in terms of the treatment phase.

By structuring and sharing the information that is produced by each area, it is expectable for the risk management to improve. Currently, there is a dataset with the reported incidents. These incidents provide an opportunity to measure the impact for the risks associated with it as well as some input to help in the evaluation of the likelihood of a risk. To do this it is necessary to associate the incidents with the risks.

DemoCorp's Information Security Incident Management AS-IS

As a requirement of ISO 27001:2013 ISIM must be performed. DemoCorp's ISIM process is relatively new in this organisation and it is being improved with the goal of making IS incidents a source of information to the organisation and improve aspects such as the accuracy of ISRM.

In DemoCorp IS incidents are reported using a digital platform. This platform offers the possibility of selecting the category of the incident to allow a prioritization for the incident response and consequently

allow a better management. This ensures that incidents that stop the production, for example, are treated with the highest priority. After this the incident is handled by the department that has the know-how to do so, which usually is the information systems department, the engineering department or the physical security department.

The IS events, including the incidents, are monthly reported to the CISO by the departments that are responsible for their treatment. These events are then consolidated into a single spreadsheet by the IS department. These spreadsheets are used to maintain historical information and to monitor the state of each incident (i.e., if the incident is already treated and verified).

Despite the existing spreadsheets there is currently no methodology to perform a systematic analysis to the occurred incidents. Furthermore, the use of separate spreadsheets and with different levels of detail difficult the ISIM learning process, since there is no explicit information in the spreadsheets to relate the incidents with the assets and relations between the assets.

The measures used to handle the incident are also described freely which means that the same measure sometimes has different descriptions, with different levels of detail, which in some cases make it very difficult to understand that they are the same.

In DemoCorp, the templates used for monthly IS incident reporting are different for each of the reporting departments and the rules and procedures for these templates are defined in different documents. Having more than one document for the same procedure is problematic as so it was proposed a unified document and template for reporting.

Step 3 - Define organisation's boundaries

The scope considered may initially consist in the assets that are directly related with the products that are forced to have ISIM and ISRM by the international standards. Then, it may expand to other assets as the ISIM process and ISRM is applied and other relations among assets are identified and classified as relevant.

Step 4 - Define security objectives

The security objectives for these products are also detailed in international standards which include, for example, network segregation, high security areas, and immediate incident report.

7.2.2. Phase B - Establish/Update EA

Step 1 - Adjust meta model

To be able to relate the concepts related with IS, the meta-model proposed in Figure 14 was used. The elements used to model the information assets and the asset resulting from control measure implementation may be seen in Figure 24. Note that, for the purpose of this research, these were the necessary elements to model DemoCorp's reality.

The code used to produce the meta-model in EAMS can be seen in the Appendix C. The code was used to implement the meta-model but it has more detail than what was represented in Figure 24 for practical purposes such as simplifying the required queries or to maintain the details from the original document.

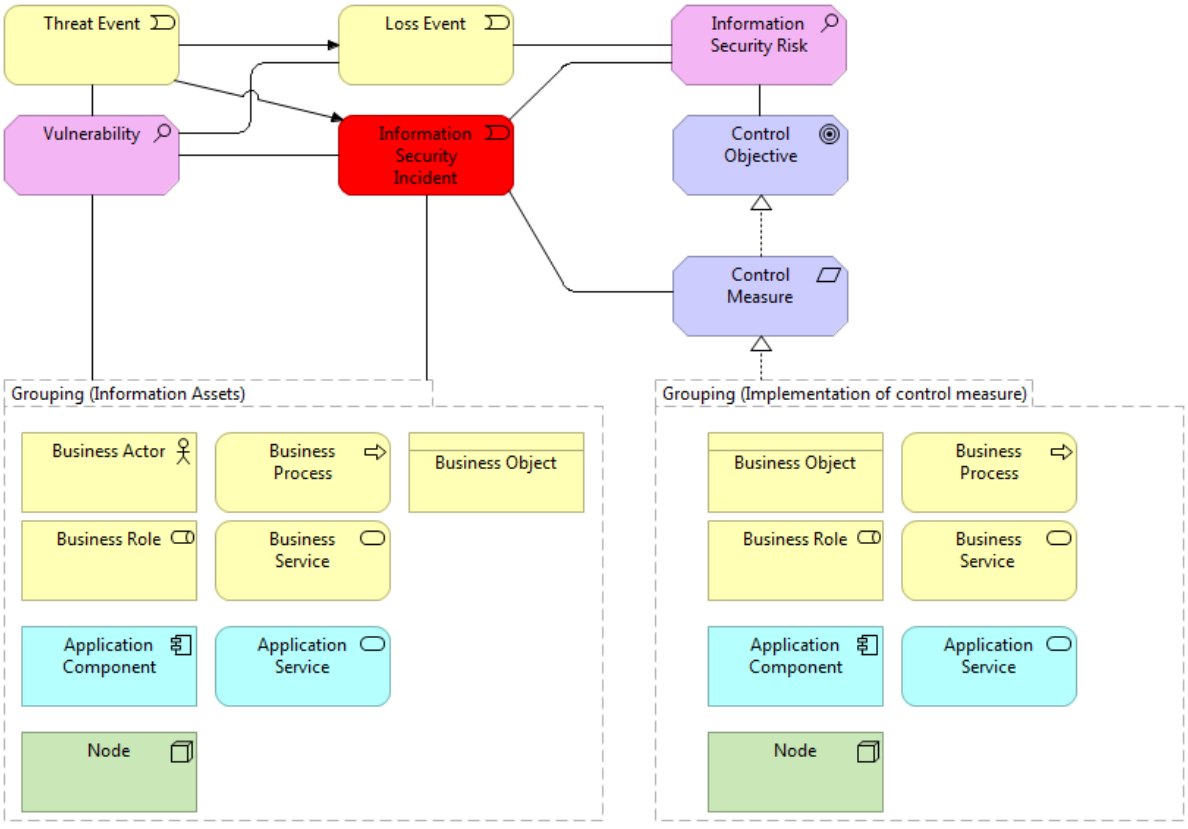


Figure 24 - Information Security Management used Meta-model

Step 2 - Identify assets

As described in section 7.2.1, asset identification is already performed as a part of risk analysis as so this information is available to be used in the context of this research. However, some transformations and additions were still necessary in terms of connections between assets, language and also asset abstraction to maintain the confidentiality of DemoCorp.

DemoCorp assets such as the external services were represented as a business service as it fits ArchiMate's description for this component. ArchiMate's business objects were used to model DemoCorp's documents, in physical and digital format. Business processes were also considered, however, the relation between the processes and the assets were not identified and it was not possible to obtain that information due to security concerns. Therefore, business processes were not used for the in this research.

Human resources were grouped by their function and therefore these groups were modelled as business roles since the definition of a business role in ArchiMate is adequate for this situation. Business actors (i.e., each employee that belongs to the group/role) were identified by DemoCorp however they will not be used for this research due to privacy concerns.

For software, DemoCorp presents two different types of group, i) groups by function and ii) groups with a single element with the application itself. The second was generalized to ease the interpretation process for a person that does not know what is the purpose of a given application.

Hardware was modelled as ArchiMate's nodes. Hardware could be modelled as specializations of nodes, however at the abstraction level that we were allowed to model it would bring no advantage since no relations were shared by DemoCorp and they were not allowed to be modelled for security reasons.

In Figure 25 it is possible to see some of the identified assets in DemoCorp.

NAME	TYPE
Data transmission	Application Service
Data transmission (test and devolopment enviroment)	Application Service
Personalization Management	Application Service
Personalization Management (development environment)	Application Service
Personalization Management (test environment)	Application Service
Proxy solution for data reception	Application Service
SLG Network share	Application Service
Solution for data preparation and personalization	Application Service
Solution for data preparation and personalization (tests)	Application Service

Figure 25 - Part of the information assets identified using EAMS.

Step 3 - Identify asset relations

DemoCorp's information was generally incomplete in terms of the relationships among assets, incidents, and risks due to the fact that identifying this relation for each event/incident is time consuming and not a straightforward process, since it currently involves looking through the entire list of identified risks in a spreadsheet. Furthermore, sometimes the IS risk list did not contain the risk associated with the occurred incident and the bureaucracy involved to its addition leads to empty cells in the spreadsheet used for monthly reports.

This is problematic since it restrains automation mechanisms to help in further analysis regarding ISRM. These relations were therefore reviewed and completed to allow a deeper analysis. Relations were then validated by the domain experts to assure their correctness.

Step 4 - Relate assets with IS risks

IS risks were obtained through DemoCorp's current ISRM process. In Figure 26 it is possible to see the interface where the relations between risks and assets is performed and updated. Note that the relationships in EAMS are bidirectional as so connecting assets to risks or risks to assets, is the same in practice.

PROPERTY NAME	PROPERTY VALUE
Name	Equipment unnavailability due to Electric Power Shortage
Asset Group ID	ID056
Associated Assets	Administrative Building Factory Building
Associated Control ID	IDC097
Associated Control Measure	Electrical Generator Maintenance contract UPS
Associated Control Objective	
Associated Loss Event	
Associated Threat Event	Electric Power Shortage
Associated Vulnerability	Lack of redundancy in the electrical power supply

Figure 26 - Relationship between a risk and two assets in EAMS.

Step 5 - Relate control measures with IS risks

The control measures were obtained through DemoCorp's current ISIM and ISRM processes. In Figure 26, it is possible to see the relation between the risk and the associated control measures.

Step 6 - Relate IS incidents with the other elements

IS incidents were obtained through DemoCorp's current ISIM process. However, the relations between assets and IS incidents and other elements were not yet thought of (e.g., the relation between IS incidents and existing controls measures or IS risks). The measures used or planned to handle the IS incidents were described, however there was no linking mechanism, such as an ID, to relate control measures and IS incidents. These relations were required for this research therefore they were identified and validated by the domain experts in DemoCorp.

In Figure 27, it is possible to see the relation between the IS incident and the affected assets, the associated control measures, and the associated risk.

PROPERTY NAME	PROPERTY VALUE
Name	Electric Power Shortage - product SLAs compromised
Affected department	
Affects	Machines type A Machines type B Machines type C Network Equipment
Associated Corrective Control Measure	Switch Replacement UPS - batteries replacement UPS - testing
Associated Corrective Control Objective	
Associated Risk	Equipment unnavailability due to Electric Power Shortage

Figure 27 - Relationship between an incident and the affected assets, the associated control measures, and the associated risk in EAMS.

7.2.3. Phase C - Perform Double-loop Learning

Step 1 - Identify incident trends / patterns

To be able to identify incident trends, it was necessary to normalize the existing data since some attributes were originally in human language (i.e., sentences were used instead of using only the necessary concepts, with different words/strings for the same concept) furthermore in some cases a spreadsheet cell contained more than one concept. Having multiple concepts in a cell implies that the information was not in the first normal form (1NF), which says that each attribute contains only atomic values [39].

Normalizing information in this context is particularly important since the objective is to be able to understand which control measures can be generalized to perform systemic corrective actions. Without this normalization, what happened was that even though some IS risks and IS incidents had the same control objectives and control measures associated with them, by having a different string describing them, it was slower to understand if the control objectives and measures were the same since it required human validation. Validating instances may bring even more difficulties in cases where the terminology used is only understood by domain experts.

The relations provided by ArchiMate were used to relate DemoCorp's assets and other IS relevant elements as seen in Figure 24. And were further approved by DemoCorp's domain experts.

To support this phase EAMS was used. This software allows to merge imported instances and consequently improve and ensure data quality as well as to support knowledge management within the organisation. This is fundamental since currently the data is not standardized, resulting in different names for the same thing due to different persons naming using their own preference, for example.

Queries were performed in EAMS using its own query language ERML which has a logic similar to SQL. In this research, the queries were used to obtain the relevant elements for each view (Blueprint) and also to define connections between these elements in the form of arrows.

The query shown in Figure 28 was used to select only the IS incidents with higher impact that are not part of a group of IS incidents. These groups were used to avoid having to much information in the blueprints and therefore making it difficult to use. This query applied over the used data results in the part of the blueprint shown in Figure 29.

```
<IQD>
  <TYPE>Information Security Incident</TYPE>
  <BLOCK>
    <WHERE>
      <FIELD>Impact</FIELD>
      <OPERATOR>gt</OPERATOR>
      <VALUE>3</VALUE>
    </WHERE>
    <AND>
      <WHERE>
        <FIELD>IsComponent</FIELD>
        <OPERATOR>==</OPERATOR>
        <VALUE>false</VALUE>
      </WHERE>
    </AND>
    <AS>V01.01</AS>
  </BLOCK>
</IQD>
```

Figure 28 - Query to obtain the IS Incidents with an impact above 3 that are not part of a group of IS incidents

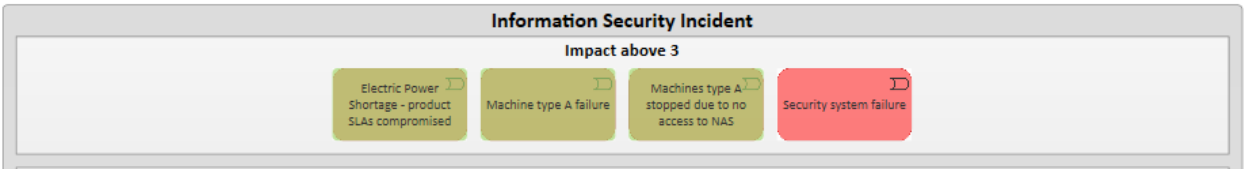


Figure 29 - Resulting Blueprint of applying the query shown in Figure 28.

The query shown in Figure 30 was used to make a connection between elements of the blueprint, this one was used to connect IS incidents and assets. To use the query in the blueprint there are some additional steps required in EAMS however they are performed using the interface and have no particular interest since these steps are simple.

```
<IQD>
  <ARG Index="1" />
  <BLOCK>
    <PROPERTY>Affects</PROPERTY>
  </BLOCK>
</IQD>
```

Figure 30 - Query used to make a connection between elements of the blueprint, this one was used to connect IS incidents and assets.

The result of the application of the query in Figure 30 can be seen in Figure 31. Figure 31 illustrates which where the IS incidents that affected a selected asset, in this case the personalization machines which gives an insight on what was able to affect this asset. Electrical power failure, mechanical problems and network problems were some of issues. This was an example, another asset could be selected by just clicking on it.

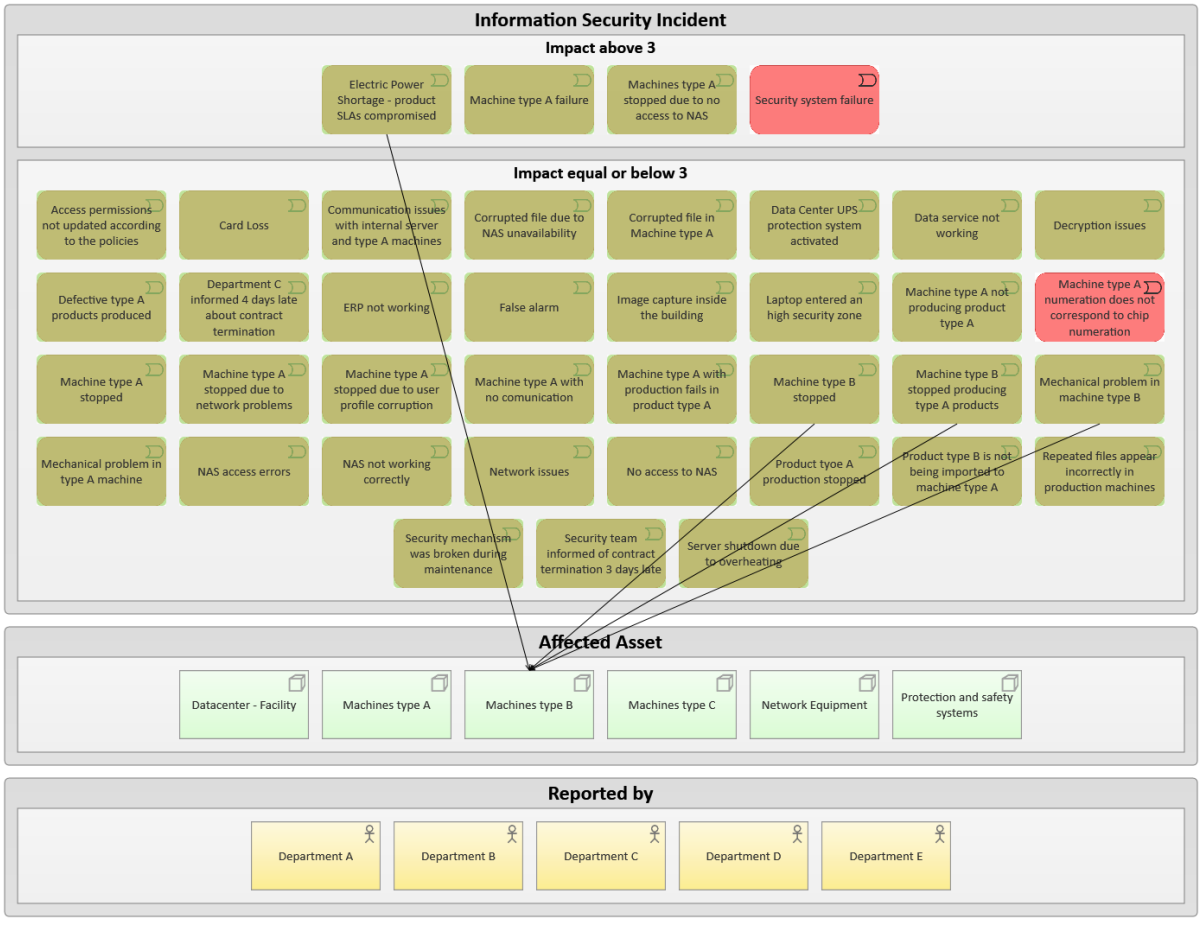


Figure 31 - Information Security Overview Blueprint - Showing the incidents that affected a particular asset.

In Figure 32 it is possible to see which incidents are solved and which are not solved yet allowing also to click in them for further details or to navigate to another blueprint focusing on the incident clicked.

Note that the incidents represented in green in the images, are incidents that were already solved while incidents represented in red are still open since no solution was found and/or implemented and/or verified.

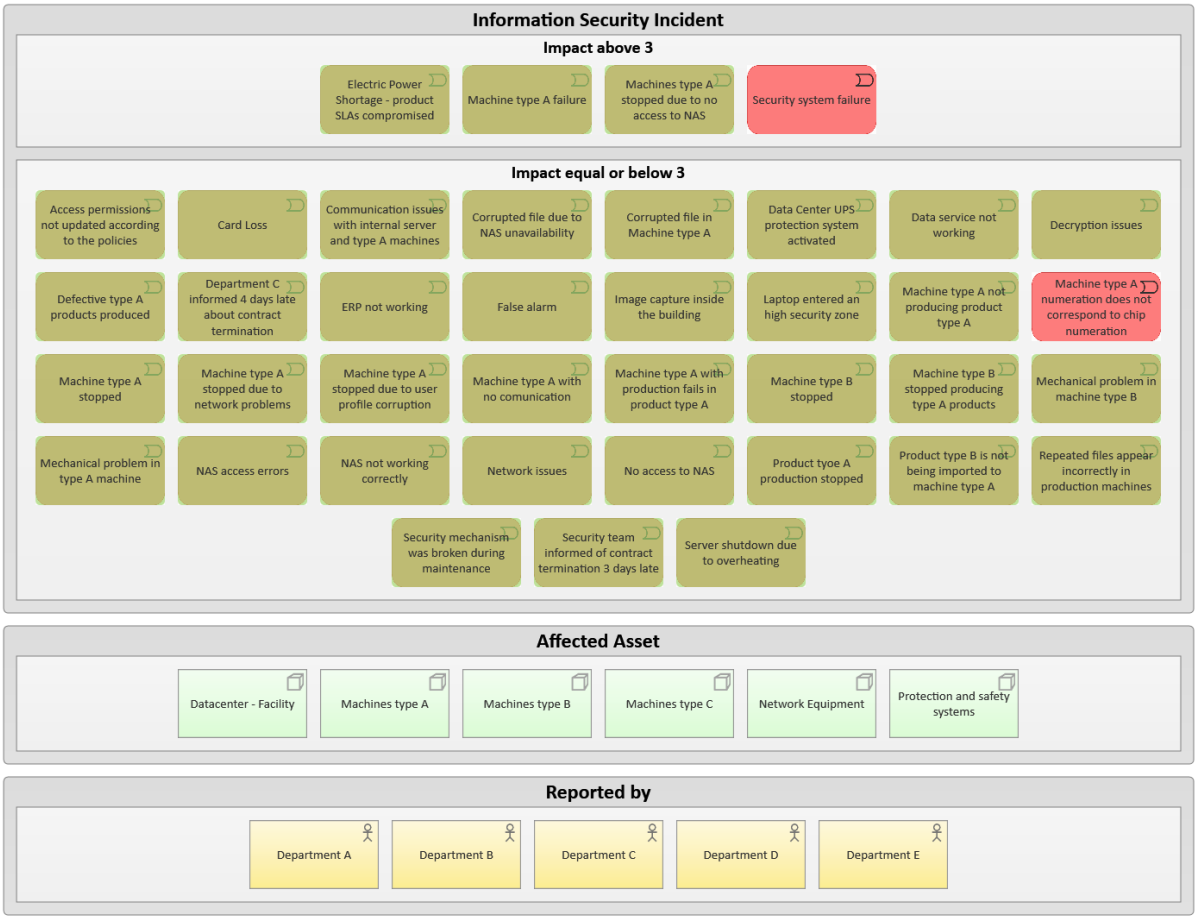


Figure 32 - Information Security Incident Overview Blueprint - Showing in red the incidents that are not treated yet.

By being able to see how vulnerabilities are being addressed at the moment it is possible to understand how the IS incident materialized (i.e., the vulnerability explored as well as the threat event that triggered the incident). This brings the mechanism necessary to be able to perform a systemic corrective action since it is possible to select a control measure with a broader scope allowing it to eliminate or reduce the likelihood of future IS incidents involving that vulnerability and/or threat event associated.

This can also be used to understand if the same vulnerability is being addressed the same way across the organisation allowing then to homogenize the solutions being used and also to communicate the best solutions, based on the historic of the organisation.

EAMS also allows navigation between blueprints. To define the navigation, it was necessary to edit the XML file used for that purpose as can be seen in Figure 33. In this figure, the XML file content regarding navigation definition may be seen. This consists in defining what happens when an element is double-clicked which is the ActionType="Default", the “trigger type” is used to distinguish between the elements that are clicked, the “origin name” has the name of the origin blueprint and the “destination name” has the name of the destination blueprint.

Being able to navigate through blueprints provides a faster way to go to the relevant blueprint. After the definition of the navigation, it is only necessary to double-click the element with interest for the current analysis to go to the destination blueprint. Considering Figure 33, if we were on blueprint “Information Security Risk” and we double-clicked in an Information Security Incident instance EAMS would present the Information Security Incident blueprint focusing on the clicked incident.

```
<?xml version="1.0" encoding="utf-8" ?>
<Navigation xmlns="http://www.link.pt/eams">
  <Profile Name="IT Architect" Default="true">
    <Origin Name="Information Security Risk" OriginType="Blueprint">
      <Action ActionType="Default" DestinationType="Blueprint">
        <Trigger Type="Information Security Incident" />
        <Destination Name="Information Security Incident" />
      </Action>
    </Origin>
    <Origin Name="Information Security Overview" OriginType="Blueprint">
      <Action ActionType="Default" DestinationType="Blueprint">
        <Trigger Type="Information Security Incident" />
        <Destination Name="Information Security Incident" />
      </Action>
      <Action ActionType="Default" DestinationType="Blueprint">
        <Trigger Type="Information Security Risk" />
        <Destination Name="Information Security Risk" />
      </Action>
    </Origin>
    <Origin Name="Information Security Incident Overview" OriginType="Blueprint">
      <Action ActionType="Default" DestinationType="Blueprint">
        <Trigger Type="Information Security Incident" />
        <Destination Name="Information Security Incident" />
      </Action>
    </Origin>
  </Profile>
</Navigation>
```

Figure 33 - Navigation between blueprints.

Considering now the trend analysis, in Figure 34 it is possible to observe that eight incidents are related with network equipment which leads to a reflection on how can the network be improved to avoid damaging the network equipment and/or to reduce the negative effects of problems with the network equipment when an incident occurs. Note that the data set used did not provide the root cause of the incidents which means that there is no information to clarify if the network equipment failure caused the incident or if the incident caused the failure in the network equipment.

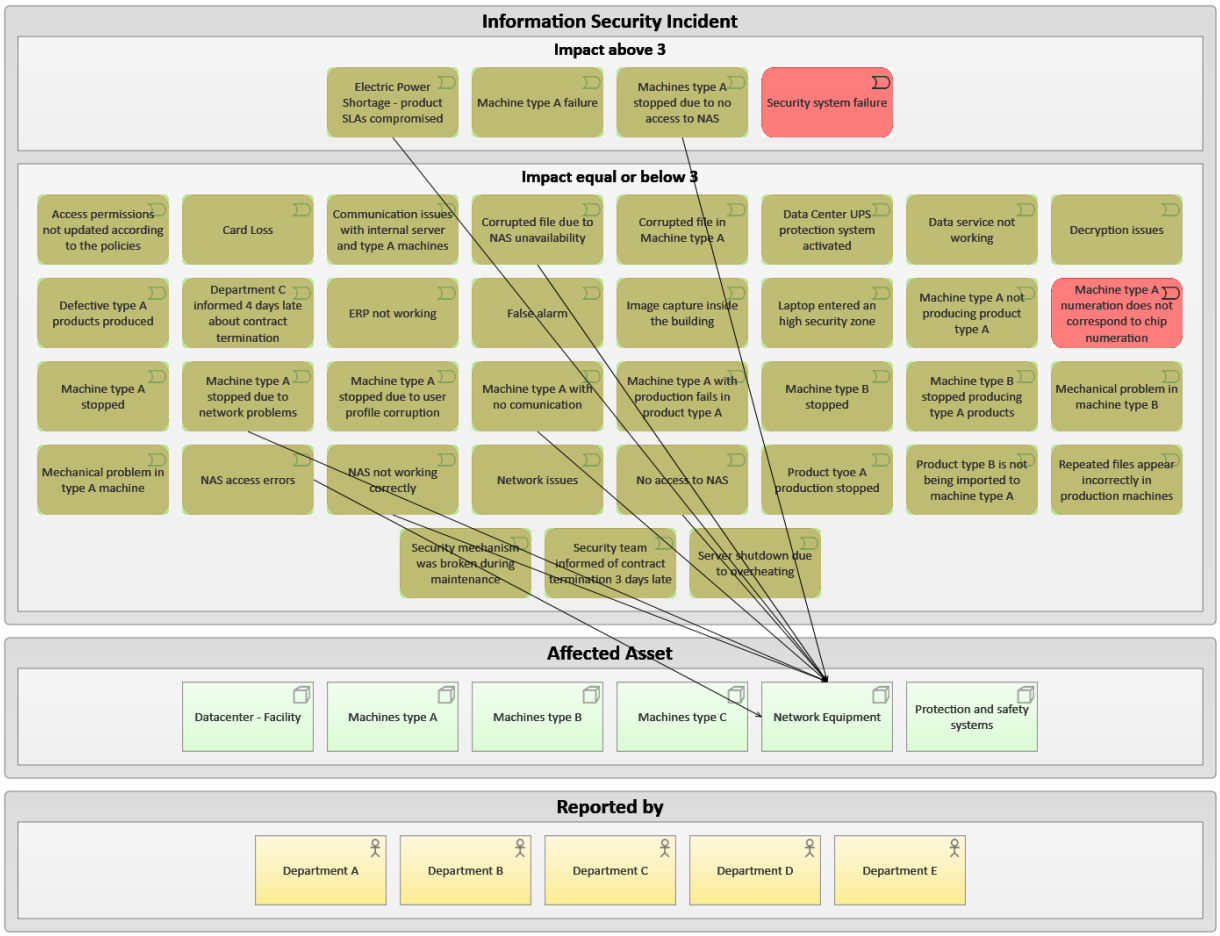


Figure 34 - Information Security Incident Overview – Showing the relations of a particular asset.

Step 2 - Identify the best control measures

Considering the trend observed in Figure 34, the control measures regarding this equipment type would be for example to use redundancy in the network equipment and an uninterruptible power supply (UPS) for the network equipment and to change the maintenance contracts to increase the frequency with which the equipment is reviewed.

Step 3 - Propose systemic corrective actions

Considering that electric power shortage is a threat and may stop network equipment and since the objective is to perform a systemic corrective action, it is important to understand which are the other assets that are exposed to electrical power shortage. As so, in Figure 35, it is possible to see which were the assets affected by the last electrical power shortage. With this observation, it is possible to understand that the datacentre and the safety systems use backup power systems. Considering this the proposed corrective action is to equip the machines type A, B and C and the network equipment with UPSs, and acquire a power generator or find a redundant power supplier.

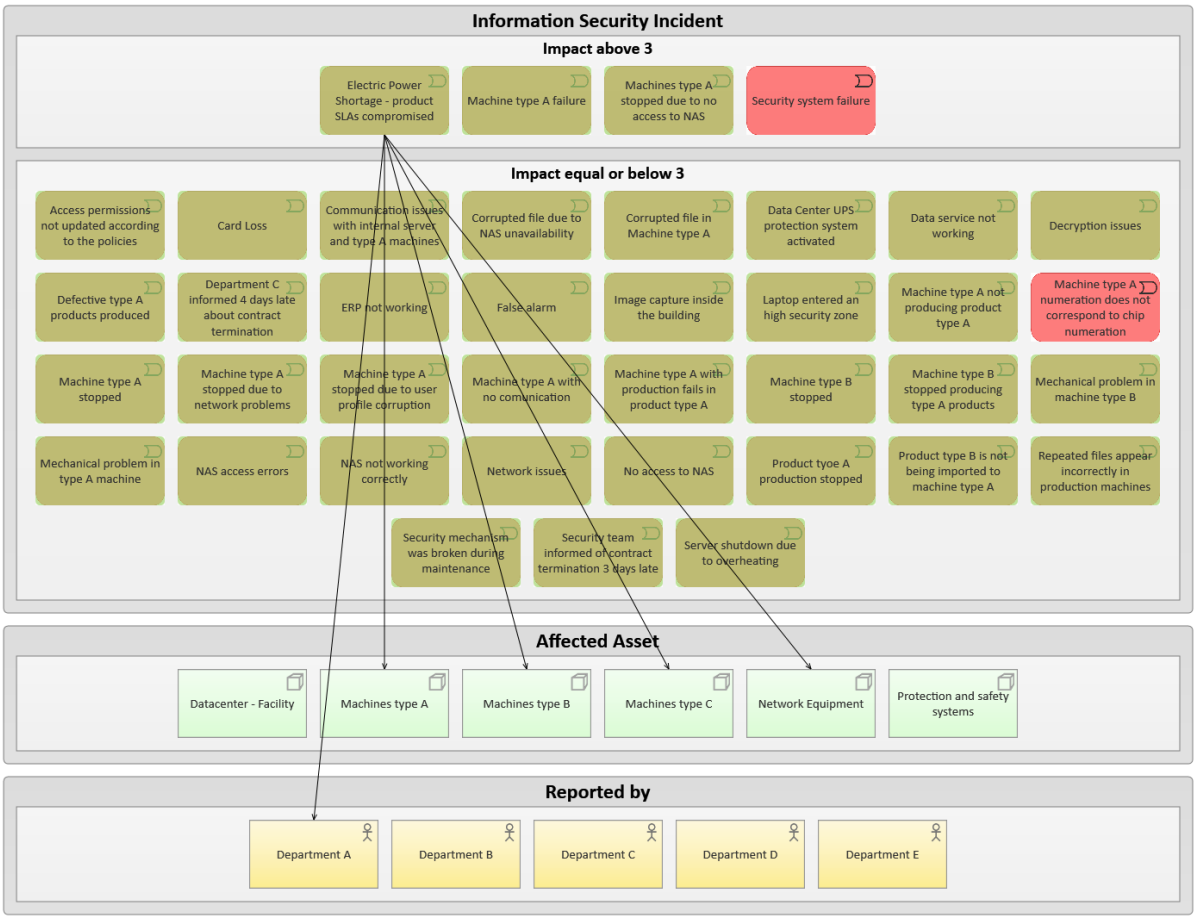


Figure 35 - Assets affected by electrical power shortage in EAMS.

Step 4 - Model the proposed corrections

Figure 36 presents the proposal described in the step 3 of this phase. To achieve this, it is only necessary to introduce which are the proposed systemic corrections related with the particular IS incident. Note that the blueprint needs to be designed but this is only performed once and can later be used for all incidents.

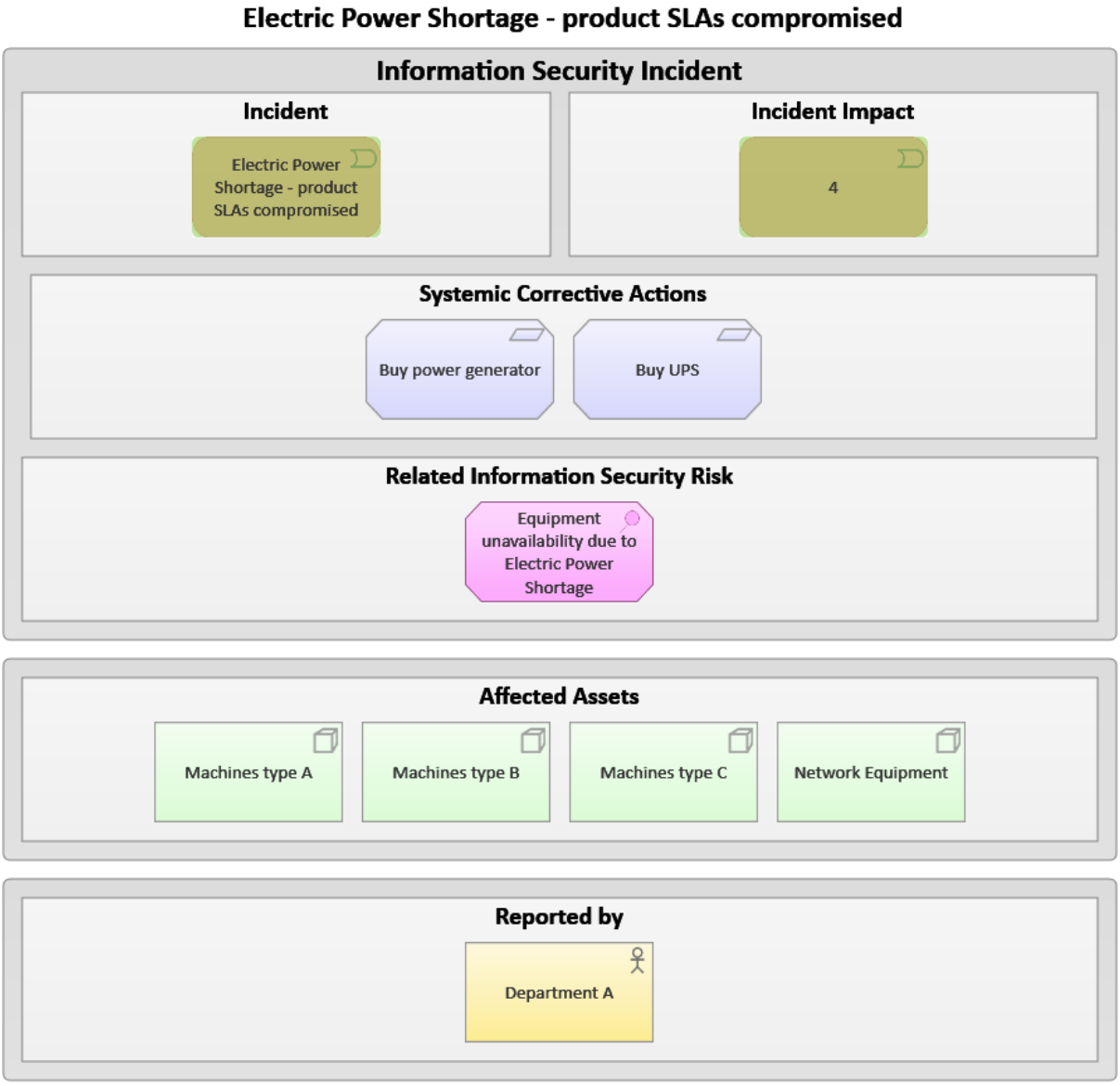


Figure 36 - Blueprint with the Systemic Corrective action proposal in EAMS.

7.2.4. Phase D - Perform Systemic Corrective Actions

Step 1 - Evaluate the proposed corrections

EA provides the support needed for planning since it allows the responsible for control definition to understand which assets should be included in order to correct the problem in the system instead of independent local solutions.

In the example presented in Figure 36 there is a summary of what was involved in this correction. Furthermore, the one responsible to evaluate may click in the proposed correction to obtain detailed information as represented in Figure 37.

PROPERTY NAME	PROPERTY VALUE
Name	Buy power generator
Associated with	
Begin Date	
Control effectiveness	
Control Measure ID	
Control Objective	
Control Owner	
Currency unit	
Description	A power generator able to support all the machines and the network equipment will cost 100000. A power generator able to support all the type A machines and the network equipment will cost 30000.

Figure 37 - Systemic Correction details

Step 2 - Choose and justify the decision

Considering the costs and the benefits of the systemic corrective action we will consider that due to budget constraints DemoCorp opted to buy a power generator just to support type A machines and network equipment since with this option it will be possible to ensure the delivery in time unless the power shortage fails for more than 10 hours in a week, which only happened once in the last twenty years.

Step 3 - Implement systemic control measures

To monitor control implementation, it is possible to use the time functionality which allows to see which controls are planned and which are already implemented. EA also helps in complex corrections however in this example it is not necessary to use it.

Step 4 - Update organisation's EA

In this example, this consists in introducing the two instances in EAMS, the UPS and the power generator and associating it he the respective risk.

Step 5 - Promote Risk assessment

After updating the EA, the security manager should promote the risk assessment and provide access to the blueprints of the risks that have changes (e.g., new control measures associated or new assets associated). In Figure 38, it is possible to observe an overview of the equipment unavailability due to electric power shortage risk.

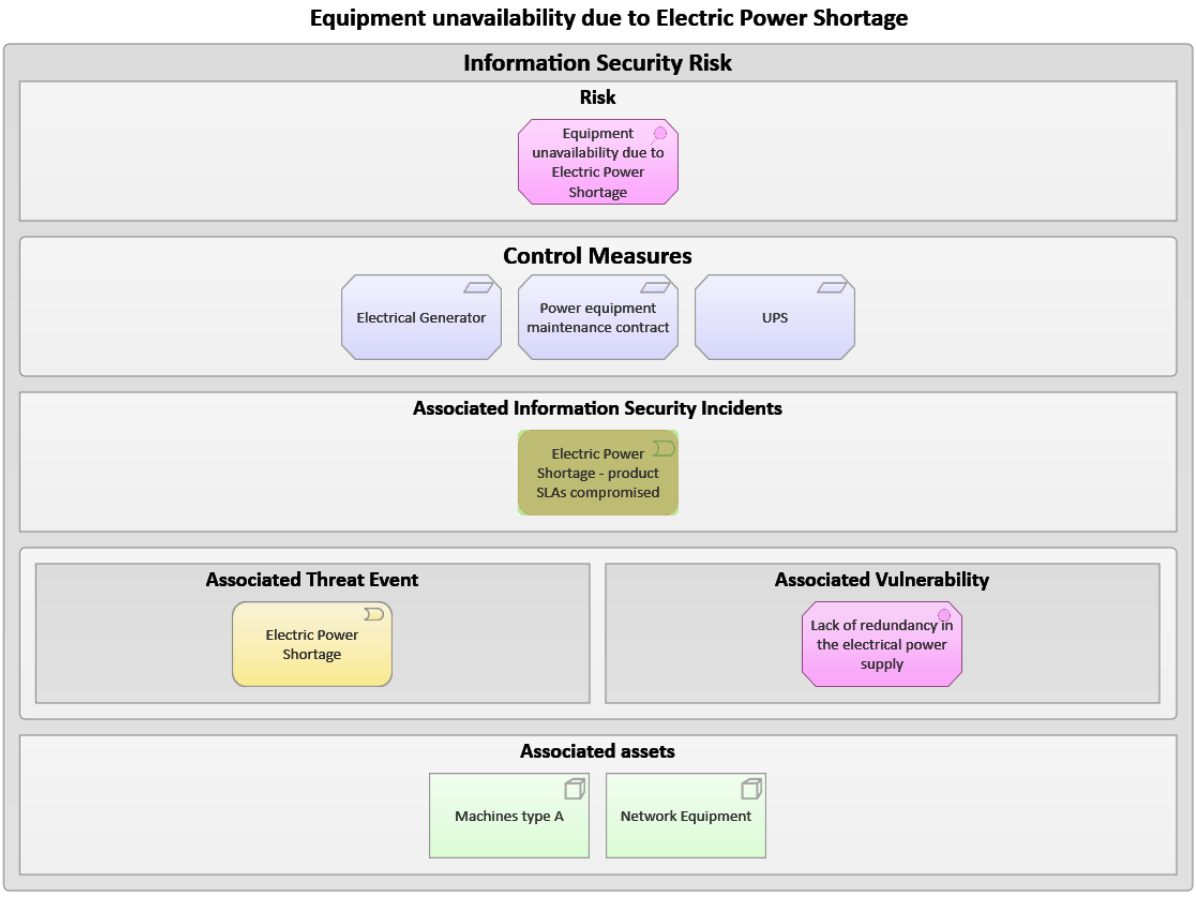


Figure 38 - Equipment unavailability due to electric power shortage risk overview

7.2.5. Phase E - Perform IS Risk Review

Step 1 - Analyze EA

Considering the corrections, it is important to re-evaluate the risk levels. The risk level may change due to the implementation of control measures or due to acknowledging the real impact of a risk, having into account the incidents that occurred related to the identified risk.

Step 2 - Identify IS risks

These risks can be better related with incidents when a visual support exists, in this case EAMS blueprints that allow to both see the connections between the represent components as well as navigate between blueprints similar to a drilldown function. With the correct configuration, it can provide support for ISRM.

In this example the implementation of two new controls, brings new risks related with the UPS batteries and the power generator since they may fail UPS. Therefore, a periodic UPS review of this equipment should be implemented. The risk of unavailability due to electric power shortage of the machines type B and type C should also be added as a separate risk since its probability and consequences will be different from the risk in machines of type A and network equipment due to the controls implemented.

Step 3 - Evaluate IS risks

In Figure 39 it is possible to see the related incidents which provides important feedback regarding the real impact of an IS incident that is no more than the materialization of an identified IS risk. Using EAMS, it is also possible to see dates in which the incidents occur to identify which control measures were implemented since the last IS risk analysis by highlighting them (the used colour was grey but it can be another one). Considering this the ISRM team should be able to calculate more accurately the risk impact.

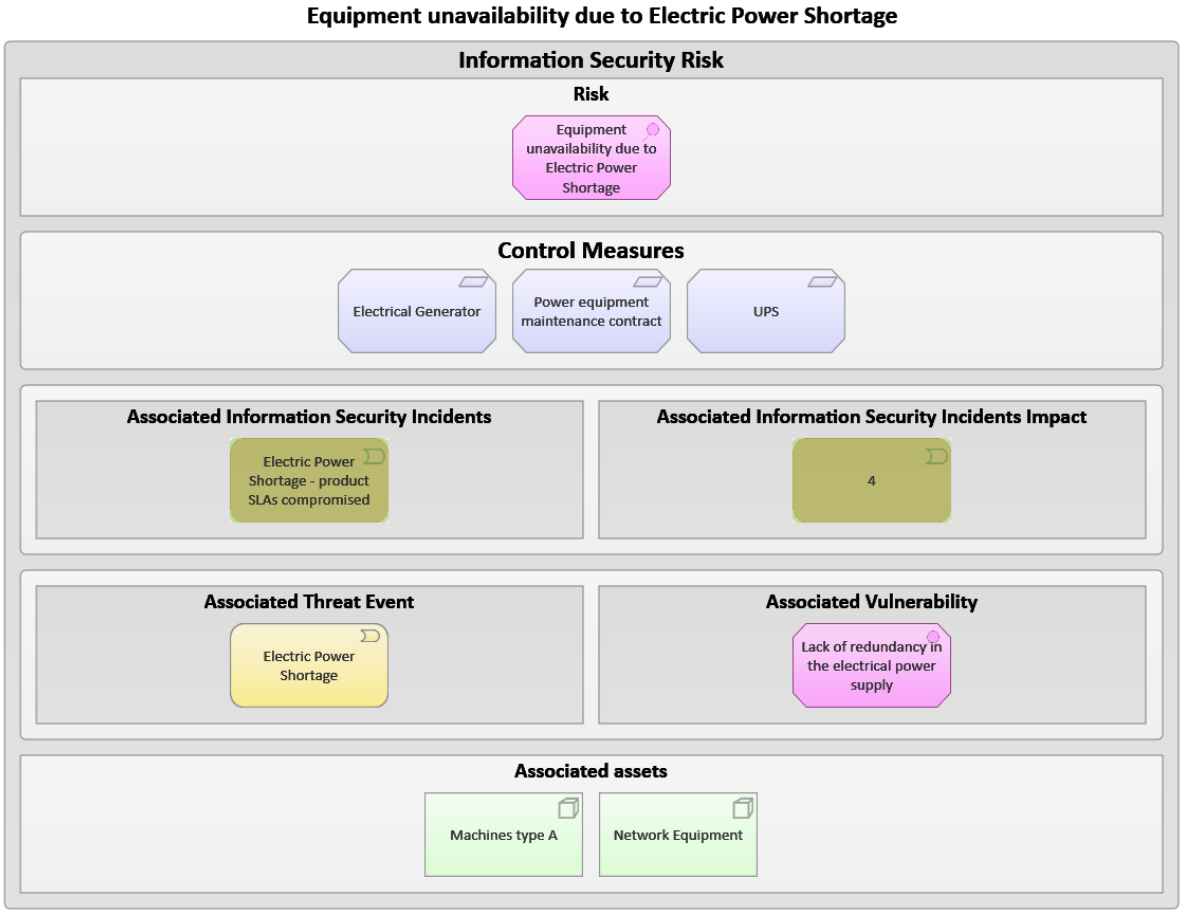


Figure 39 - IS Risk blueprint showing IS incident impacts

8. Evaluation

This section is aligned with the evaluation activity of DSRM and explains how the proposed solution will be evaluated. This evaluation will consist in analysing the benefits that the proposed methodology brings to DemoCorp comparing the advantages and disadvantages the current process of ISIM and the proposed methodology.

8.1. DemoCorp Identified Benefits

DemoCorp benefits were mainly in terms of ease of visualization of the affected assets for each incident as well as the related risks. In practice, this means that now it is possible to evaluate risk's probability and impact with better accuracy due to the capabilities to explore historic.

Using the proposed methodology, it was possible to rapidly identify that despite the existence of control measures for some IS risks, related IS incidents still occurred. This implies that these control measures must be revised and indicates that it is easier to analyse using the proposed methodology and tools than the ones being used at DemoCorp.

The controls are implemented over time, being able to see when the controls were implemented or when they are planned to be implemented helps to avoid redundant controls or conflicts between them, as mentioned by a member of DemoCorp's ISRM team.

It is also easier to justify the predicted costs associated with the implementation of a control, since the context in which the control will act, is easily explored by navigating between related assets.

8.2. Comparison between solutions

To be able to understand the value of the proposed solution, in this section it is compared with the currently used solution (i.e., multiple spreadsheets); eramba (community version); and ArchiMate with a modelling tool such as Archi. The criteria used correspond to the list of identified aspects that differ between the different approaches, these criteria are explained in Table 5. The comparison performed in **Table 6** is based on practical experience using the tools mentioned.

Table 5 - Criteria description.

Criterion	Explanation
Attack vectors	Capacity to represent attack vectors.
Automatisms	Automatisms offered by the tool.
Communication between teams	Support provided to ease the communication.
Connection between IS incidents and IS risks	Supported connection types between the two domains.
Cost	Costs associated with software licenses and human resources capable of working with it.
Data Normalization	Support provided to normalize data.
Data quality assurance	Support provided to ensure data quality.
Effort to maintain updated	Effort to ensure that the information is up to date, coherent, and useful.
Helps with complexity	Support to abstract irrelevant information for a given analysis.
Holistic view	Support mechanisms to be aware of the whole organisation.
Initial effort	Effort necessary in the first iteration of the methodology.
Learning supporting capabilities	Support to retain relevant information in a format that is easy to consult.
Lifecycle	Support to analyse incidents', risks', and assets' lifecycle.
Personalized view	Support to produce different views of the same reality.
Time analysis	Support to analyse time intervals.

Using the criteria previously described, different approaches to support systemic corrective actions were analysed to understand how they may support these actions and enable efficient communication between ISIM and ISRM teams. In Table 6 there is a summary that overviews the advantages and disadvantages of each approach. To explain the classifications, the rational is detailed on the next paragraphs.

Table 6 - Comparison between the proposed methodology and existing approaches.

Classification: 1- very bad; 2- bad; 3 – good; 4 - very good.

	Spreadsheet	Eramba	Proposed Methodology Archi	Proposed Methodology EAMS
Attack vectors	1	1	4	4
Automatisms	2	3	1	4
Communication between teams	1	2	4	4
Connection between IS incidents and IS risks	1	1	4	4
Cost (licenses + employees)	4	3	2	1
Data quality assurance	1	4	1	4
Data Normalization	1	4	1	4
Effort to maintain updated	1	4	1	4
Helps with complexity	2	2	3	4
Holistic view	2	2	3	4
Initial effort	3	4	2	1
Learning supporting capabilities	2	2	3	4
Lifecycle	2	2	3	4
Personalized view	2	1	2	4
Time analysis	4	1	1	4
Total	29	36	35	54

Attack vectors are difficult to represent in a spreadsheet in a way that makes easy to understand the relation between assets, which leads to great effort to analyse incidents that affect multiple assets. Eramba goes a little further and helps to visualize which assets were affected however the relations between the assets do not exist which may lead to difficulties understanding the flow of an attack or that an asset failed because it depends on other that also failed. Using a modelling language such as ArchiMate or the modelling mechanisms of EAMS it is possible to represent these relations and flows therefore improving the information that can be summarized in one view/blueprint and consequently reducing the effort to understand it.

Automatisms in spreadsheets regarding asset and incident representation do not exist by default. It is possible to programme them to work similar to a relational database however, the effort to achieve this is considerable. Additionally spreadsheets lack explicit metadata which makes difficult to join or integrate data across multiple spreadsheets [40] which is necessary to relate assets for example considering the Second Normal Form (2NF) that force the non-prime attributes of the relation to be dependent of the whole candidate key [41] for example. Eramba provides some automatisms regarding pie charts related to the incidents and the existing risks as well. ArchiMate modelling tool Archi does not provide any relevant automatism to this research other than ensuring that ArchiMate relationship rules are being followed. EAMS provides interesting features such as blueprint generation that allows the generation of new blueprints as data is updated without any effort to the user, it is also capable of providing charts and other features such as data integration mechanisms and data update.

Communication between teams is difficult with a spreadsheet when there are multiple tables and/or many columns. It is both unappealing and difficult to use even using filters and hiding columns. Eramba is helpful for monitoring IS incidents, risks and compliance, however it does not provide mechanisms to simplify the IS incidents to ease the task of learning/discuss about them in its context. Archi is good for this purpose, the views/blueprints may be designed to abstract unnecessary details for a given analysis or discussion. EAMS is good for this purpose, the views/blueprints may be designed to abstract unnecessary details for a given analysis or discussion. EAMS provide further capabilities regarding automatic blueprint generation and the possibility to drill down into element details without the need to apply multiple filters and manually hide/unhide columns.

Connection between IS incidents and IS risks is unidirectional in spreadsheets and eramba, and bidirectional in ArchiMate and EAMS. In spreadsheets, associations are represented one per row. Furthermore, it is necessary to use two sheets to access the risks related to one incident, the risk's table and the incident's table (supposing the 2NF) and apply filters to obtain an understandable view. In eramba it is not possible to have a view with the IS incidents related with a given IS risk. In ArchiMate and EAMS it is possible to see which risks are associated with an incident and which incidents are related to a risk in a single view.

Regarding costs, there are open source spreadsheets, however, it is necessary some knowledge about spreadsheets programming to be able to ensure correctness of the data since spreadsheets by itself do not ensure that incidents and risks relationships are defined correctly and the fact that they should be in different sheets or tables forces to use some restrictions in the spreadsheet to ensure coherence. Eramba has some free features that are enough to register IS incidents and some paid features that allow personalization regarding which attributes should be registered. To be able to adjust this tool to support systemic corrective actions as proposed in this research, it is necessary to use the paid version. However, the people that use the tool is not required to be able to programme as eramba offers an easy interface to personalize which attributes are registered. Archi is open source but requires a person with

knowledge regarding EA and ArchiMate to be able to use it correctly. EAMS has a monthly subscription and requires a person with knowledge regarding EA and SQL at least.

Data Normalization is not possible to ensure in a spreadsheet using the embedded features. Eramba offers mechanisms to make it easier such as default columns that are normalized if no personalization is performed. Archi has no mechanisms to ensure it. EAMS offers mechanisms to make it easier such as instance merge and update. EAMS is also useful regarding normalization because it the data is not normalized at least in the 2NF it is very hard to produce coherent blueprints.

Data quality assurance in spreadsheets is not a trivial task since an update in a row may force the change of multiple rows which referred to the same attribute and unless the data was previously normalized this is not possible, repeated lines or redundant terms are also common errors. Eramba helps to improve data quality when compared to a spreadsheet since the different data types are linked (i.e. changing an asset name only needs to be done once, and not for every row mentioning it as in a spreadsheet). Archi has no data quality assurance mechanisms. EAMS introduction of data implies connections which leads to better results due to the fact that it is possible to see each elements of a given data type already exist (e.g., when introducing an IS incident related IS risks it is possible to see from a list or through the autocomplete function while typing what exists already avoiding term redundancy). It also allows to edit and merge instances which avoids, for example, changing an IS Risk multiple times for example when its probability was considered to be less likely due to a control implementation.

The effort to maintain the data updated in a spreadsheet is high. When introducing new elements, it may be necessary to update multiple rows or sheets and be careful to ensure coherence. The observed tendency was that redundant information was used to simplify the consultation which leads to inconsistencies in some cases. In eramba the effort is low, the data is linked in the tool, which makes adding or editing previously inserted data easy. In Archi, the effort is very high, each update may lead to the need of changing completely a currently existing view (i.e., drag and drop multiple elements to make sure that the view is appealing and legible). In EAMS the effort is low, when identifying relations between elements, the autocomplete features help to ensure consistency avoiding redundant names for the same element. It allows decentralized updates which helps to ensure an updated model. It also allows different update modes based on data integration it is possible to do incremental updates to add a new column in multiple instances of a type of asset for example.

In terms of support to handle complexity a spreadsheet does not help since analysing relations using spreadsheet rows and charts becomes difficult when the need to use more than one sheet arises. Eramba provides pie charts with statics such as the impact level automatically which is also possible to do in spreadsheets. Archi and ArchiMate do help with complexity by simplifying the reality showing only the relevant aspects for the IS incidents and risks for a given analysis. EAMS provides visual capabilities

that help to reduce the effort necessary to understand the relations between elements due to the blueprints that are automatically generated based on the existing data and the design defined.

In terms of the holistic view capabilities both spreadsheets and eramba offer no support since it is hard to abstract the detail and analyse the organisation as a whole to be able to perform effective systemic corrections. Archi and EAMS do help in this aspect since the they represent the existing flows inside the organisation and that helps to understand the organisation in terms of the dependencies among assets. EAMS offers further advantages in this aspect since it allows drill down on the assets and navigation between views/blueprints.

Initial effort in spreadsheets is low since it is only mandatory to define what needs to be registered and fill the corresponding fields. Eramba has a very low initial effort since the tool has some fields pre-configured to allow risk and incident management. Archi has a very high initial effort since it is necessary to define the meta model, define views, and design the views. EAMS as a high effort since it is necessary to define the metamodel, load data, and define blueprints.

Learning supporting capabilities in spreadsheets are essentially charts that help to visualize data however regarding the relations between elements is difficult to see when these elements belong to different sheets. Eramba is similar to a spreadsheet but has pre-defined pie charts. When using Archi, by understanding how the assets are related it is easier to understand how control measures can be generalized and what is the scope that each control measure should have as well as to understand which control measures contribute to a control objective for example. The incidents work as an input to alert for the need to review control measures and control objectives and consequently the risks. EAMS brings the same advantages as Archi plus the possibility to drill down on the elements such as incidents or navigate between views which speeds up the analysis.

Lifecycle can be represented in spreadsheets, eramba, Archi, and EAMS. However, it is much easier to understand the implications of an asset change in the lifecycle using Archi or EAMS than in a spreadsheet due to the explicit relations present in the views/blueprints.

Personalized views in spreadsheets do not exist however it is possible to hide columns and using charts is possible however spreadsheets are not designed to execute queries that imply different tables. Eramba does not support personalized views. Archi does support personalized views however they require a lot of effort since it is necessary to do the view manually. EAMS supports personalized views, using blueprint designer it is possible to configure a view that meets the needs, showing only the relevant elements and connections to the analysis using queries.

Time analysis in spreadsheets is possible using filters. In eramba it is not possible. Archi does not support also time analysis. EAMS supports time analysis with an embedded mechanism, a bar in the blueprint view that allows to analyse through time. Using time analysis, it is possible the quickly

understand which control measures are currently in use, which were the measures added since the last risk evaluation and the same is true for IS incidents (i.e., which incidents happened since the last risk analysis).

8.3. Lessons Learned

From Table **6**, there are some important aspects that should be kept in mind. For one side, the effort of representing and maintaining an EA is high and requires someone with know-how regarding EA. So, if an organisation objective regarding IS incidents is just to register them, a spreadsheet is enough. However, if the objective is to be able to deeply understand the implications of an IS incidents EA is useful since it enables an abstraction of the assets and the relations between them which helps to identify the potential affected assets and measures to address the IS incident that are more effective, since these measures will have a higher probability to address the right scope.

To be able to maintain the EA updated tools such as EAMS are recommended to avoid the need to generate manually a view for each IS incident. Also for a register to be useful as a learning tool it is important to be able to access its information easily. This is possible using EA, and even easier when using EAMS since visual links between assets (that can be shown or hided when clicking in EAMS blueprint elements).

9. Conclusion

Through the analysis of literature related with ISIM it was identified that organisations have difficulty performing systemic corrective actions despite recognizing their value. As so, in this research the focus was to support these actions by creating a methodology that supports their implementation and monitorization, as well as to communicate the systemic corrections to the relevant parties such as the ISRM team.

With this in mind, in this research, techniques that are potentially useful were identified, such as representations of attack vectors, ADTrees, and EA. A comparison between these techniques was performed and EA was considered to be better for the purpose of this research. Despite the fact that EA presents capabilities that are useful for ISIM's systemic corrective actions, it wasn't found previous research connecting these two ideas. Therefore, to improve corrective capabilities, as well as support ISIM and ISIRM communication, we proposed a methodology capable of responding to organisational needs in terms of continuous improvement that supports systemic corrective actions by using EA.

The methodology described is capable of responding to organisational needs in terms of continuous improvement by performing systemic corrective actions using EA to improve corrective capabilities, as well as support ISIM learning phase. To do this, the proposed methodology has five phases that include the scope definition, the development and improvement of EA and its usage to support systemic corrective actions, by analysing the connections between assets, IS risks, IS incidents, and other IS elements, as well as to improve the communication between ISIM and ISRM and other interested parties by clarifying the systemic changes performed or proposed.

We used a new approach that makes use of existing tools and techniques to support ISRM and ISIM in an integrated way providing additional capabilities in terms of analysis as well as reduced efforts in medium and long-term due to the pre-configuration of necessary views.

This research resulted in a methodology that uses EA to support ISIM learning phase and with that help to implement control measures within the right scope and able to avoid incidents related with the ones that happened in the past.

9.1. Communication

Communication is part of DSRM and aims to communicate the problem, the artefact, as well as its value to researchers and other relevant audiences [10].

With that in mind, a paper titled "Using Enterprise Architecture to Support Systemic Corrective Actions based on Information Security Incident Management" based on this research was submitted to the 20th

International Conference on Enterprise Information Systems explaining the proposed methodology to support ISIM learning phase and systemic corrective actions in organisations.

9.2. Contributions

The main contributions of this research are: the proposed methodology to support systemic corrective actions, the EA metamodel that includes IS incidents, and the proposed configuration of EAMS that enables it to be used as a ISIM tool with benefits regarding analysis capabilities and communication between different teams.

Reporting IS incidents is not a trivial task within an organisation due to the fact that in theory everyone should report the identified IS events and incidents, however people have different domains of expertise. Employees without basic knowledge about relational databases for instance may have difficulties understanding things like the importance of using an ID to identify one asset, and consequently use names instead of IDs which does not serve the purpose of relating IS incidents with the affected assets and generates problems regarding data quality since the same asset is reported with different names.

Furthermore, using EA combined with a tool such as EAMS brings advantages regarding information management in the sense that it is easier to identify the relations with assets comparing to what is currently performed in DemoCorp (i.e., looking in a different spreadsheets). When compared with spreadsheets EAMS avoids errors in the data provided or lack of data due to the difficulty in finding or understanding what is required by the ones responsible for IS incident reporting within the organisation.

It also works in cooperation with tools that are already used by organisations such as spreadsheets for registering assets, IS risks and IS incidents in the sense that what currently exists in these spreadsheets can be imported to EAMS using its embedded data integration mechanisms and the data added in EAMS may also be exported to a spreadsheet.

Being able to navigate through blueprints provides a faster way to analyse the information that an organisation possesses regarding their assets, incidents and risks.

The blueprints presented only require effort in its definition, once the relevant elements and connections are defined, it is only necessary to add more instances and the connections between them, meaning this that the visual part is automatically generated.

EA may be used as the common language to address IS and the proposed meta-model provides an approach that can be explained to the ISIM and ISRM teams easily using the visual support provided by ArchiMate. The proposed meta-model is important in the sense that it simplifies the concepts used by clarifying how the concepts are linked and how an incident report may lead to an improvement in the

organisation. Understanding the objective and importance of a task is an important step to achieve good results and involvement in it. In DemoCorp, the alienation from IS issues by some departments was experienced and being able to summarize ISIM and ISRM in an interconnected way present a support tool for improving this situation.

Regarding systemic corrective actions, being able to see the affected assets and how those assets are connected is an important support when deciding which control measures should be implemented to achieve a systemic correction. It is also expected that the proposed methodology will help to reduce the number of incident re-incidences by supporting the learning from IS incidents.

This methodology when used with the proposed tools also helps to plan the systemic corrective actions by clarifying the involved assets. The temporal feature exposed may also be used monitor the control implementation and easily understand the implications of an implementation delay.

For organisations, this research presents an alternative and/or complement to their ISIM process that is explained step by step and offers the necessary knowledge to take advantage of EA as an ISIM tool.

9.3. Limitations

To avoid confidentiality issues the data used was limited to groups of assets which restricted some important relations to be shown.

The demonstration was performed only in one organisation which means that some parameters used may be overly tuned to the demonstration.

Naming rules need to be defined in order to extract value from what is represented in the blueprints otherwise the elements in the view will not be understood and consequently the blueprint will be useless. In a spreadsheet, naming rules are also important but not as important since when using a spreadsheet, usually there are multiple columns for each row which helps to detect situations when one incident or asset is referred with multiple names.

Due to time and organisational constraints, it was not possible to apply the methodology in DemoCorp and implement the proposed control measures that resulted from the application of the methodology to the data provided.

The proposed methodology does not propose a systemic corrective action automatically or improve IS by itself. It is necessary for IS related departments to use the methodology, the proposed meta-model, and tools such as EAMS as a support to ease decisions regarding IS, improve communication capabilities and IS awareness inside an organisation.

9.4. Future Work

In future work, it would be useful to use the proposed methodology in an organisation that currently uses another approach to manage IS incidents to understand how flexible the proposed solution is. As mentioned in section 9.3 the methodology was used with the data of only one organisation due to the time constraints regarding a master's dissertation.

Another possibility is to use the proposed meta-model to help in the evaluation of an incident impact by understanding the affected assets and the value of each one which can be associated with them.

The proposed methodology scope is within the IS scope, therefore, not all incidents contributed to improve the risk model and only security related risks were identified. In the future, it would be interesting to extend the scope of the incidents and risks to enterprise risks and the incidents to other types of incidents (i.e., other than IS incidents). The quantification of the benefits obtained by using the methodology and the association of those benefits with their respective costs for implementation and returns/savings are also important topics for future research.

References

[1] ISO/IEC, “ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary.” 2014.

[2] P. S. Requirements, “Card Production and Provisioning Physical Security Requirements,” no. December, 2016.

[3] ISACA, “COBIT 5 for Information Security.” 2012.

[4] D. Cannon and D. Wheeldon, “ITIL Version 3 - Service Operation.” 2007.

[5] M. Castells, “The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume I,” *Wiley-Blackwell*. 2010.

[6] K. Laudon and J. Laudon, “Management Information Systems.” Pearson, p. 672, 2016.

[7] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, “Incident response teams - Challenges in supporting the organisational security function,” *Comput. Secur.*, vol. 31, no. 5, pp. 643–652, 2012.

[8] A. Ahmad, S. B. Maynard, and G. Shanks, “A case analysis of information systems and security incident responses,” *Int. J. Inf. Manage.*, vol. 35, no. 6, pp. 717–723, 2015.

[9] A. Hevner, S. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Q.*, vol. 28, no. 1, 2004.

[10] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–78, 2007.

[11] V. Vaishnavi and B. Kuechler, “Design Science Research in Information Systems,” *Assoc. Inf. Syst.*, 2004.

[12] A. R. Hevner and S. Chatterjee, “Design Science Research in Information Systems,” *Assoc. Inf. Syst.*, pp. 1–9, 2015.

[13] D. Cooke, M. Dubetz, R. Heshmati, S. Iftody, E. McKimmon, and J. Powers, “A Reference Guide for Learning from Incidents in Radiation Treatment.” 2006.

[14] R. Shirey, “‘Internet Security Glossary’, RFC 2828, DOI 10.17487/RFC2828.” 2000.

[15] ISO/IEC, “ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements.” 2013.

[16] I. A. Tøndel, M. B. Line, and M. G. Jaatun, “Information security incident management: Current practice as reported in the literature,” *Comput. Secur.*, vol. 45, no. SEPTEMBER, pp. 42–57, 2014.

[17] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2.” 2012.

[18] ISACA, “CyberSecurity Nexus.” 2015.

[19] ISO/IEC, “ISO/IEC 27035: Information technology - Security techniques - Information security incident management.” 2011.

[20] ENISA, “Good Practice Guide for Incident Management,” *Eur. Netw. Inf. Secur. Agency*, 2010.

[21] A. Jones, “Catching the malicious insider,” *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 220–224, 2008.

[22] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, “Sharing information on computer systems security: An economic analysis,” *J. Account. Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[23] A. Ahmad, S. B. Maynard, and G. Shanks, “A case analysis of information systems and security incident responses,” *Int. J. Inf. Manage.*, vol. 35, no. 6, pp. 717–723, 2015.

[24] ISO - The International Organization for Standardization, “ISO 31000: Risk management - Principles and guidelines.” p. 24, 2009.

[25] D. L. Cooke and T. R. Rohleder, “Learning from incidents: from normal accidents to high reliability,” *Syst. Dyn. Rev.*, vol. 22, no. 3, pp. 267–271, 2006.

[26] ISO/IEC, “ISO/IEC 27005: Information technology — Security techniques — Information security risk management.” 2011.

[27] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and O. H. Longva, “A framework for incident response management in the petroleum industry,” *Int. J. Crit. Infrastruct. Prot.*, vol. 2, 2009.

[28] C. McNamara, “Field Guide to Consulting and Organizational Development: A Collaborative and Systems Approach to Performance, Change and Learning,” *Authenticity Consulting*. 2006.

[29] European Network and Information Security Agency (ENISA), “ENISA Threat Landscape 2015,” no. December, pp. 67–70, 2016.

[30] T. Ingoldsby, *Attack Tree-based Threat Risk Analysis*. 2013.

[31] & S. T. Ekstedt, M., “Enterprise architecture models for cyber security analysis. Paper presented at the Power Systems Conference and Exposition, 2009. PSCE’09. IEEE/PES.,” 2009.

[32] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, “Attack – Defense Trees ⋆,” pp. 1–38, 2012.

[33] J. W. Ross, P. Weill, and D. C. Robertson, *Enterprise Architecture as Strategy - Creating a Foundation for Business Execution*. 2006.

[34] ISO/IEC/IEEE, *ISO/IEC/IEEE 42010: Systems and software engineering -- Architecture description*. 2011.

[35] I. Band, W. Engelsman, C. Feltus, S. G. Paredes, J. Hietala, H. Jonkers, and S. Massart, “Modeling Enterprise Risk Management and Security with the ArchiMate Language,” *Open Gr.*, p. 40, 2014.

[36] F. Innerhofer-Oberperfler and R. Breu, “Using an enterprise architecture for IT risk management,” *Issa*, pp. 1–12, 2006.

[37] National Institute of Standards and Technology, “Managing Information Security Risk,” *NIST Spec. Publ. 800-39*, no. March, 2011.

[38] The Open Group, “ArchiMate 3.0 Specification.” 2016.

[39] E. & Navathe, *Sistemas de Banco de Dados*, vol. 6ed, no. 9. 2013.

[40] Z. Chen, M. Cafarella, J. Chen, D. Prevo, and J. Zhuang, “Senbazuru: A Prototype Spreadsheet Database Management System,” *Proc. VLDB Endow.*, vol. 6, no. 12, pp. 1202–1205, 2013.

[41] W. Kent, “A simple guide to five normal forms in relational database theory,” *Commun. ACM*, vol. 26, no. 2, pp. 120–125, 1983.

Appendixes

Appendix A: Threat Agents and Top Threats

Table 7 - Involvement of threat agents in the top threats from [29]**.**

	Threat Agents								
	Cyber criminals	Insiders	Online social hackers	Nation States	Corporations	Hacktivists	Cyber Fighters	Cyber terrorists	Script kiddies
Malware	✔	✓	✓	✔	✔	✓	✓	✔	✓
Web-based attacks	✔			✔	✔	✔	✔	✔	✔
Web application attacks	✔			✔	✔	✔	✔	✔	✓
Botnets	✔			✓	✓	✔	✔	✔	✓
Denial of service	✔			✔	✔	✔	✔	✔	✔
Physical damage/ theft /loss	✓	✔		✔	✔			✔	
Insider threat	✓	✔		✓	✓			✔	
Phishing	✔	✓	✔	✔	✔	✔	✓	✔	✓
Spam	✔		✔	✓	✓	✓	✓	✔	✓
Exploit kits	✔			✔	✔	✓			✓
Data breaches	✔	✓		✔	✔	✔	✔	✔	✔
Identity theft	✔	✔		✔	✔	✔	✔	✔	✓
Information leakage	✔	✔	✓	✔	✔	✔	✔	✓	✓
Ransomware	✔		✓						✓
Cyber espionage		✓		✔	✔				

Legend:
Primary group for threat: ✔
Secondary group for threat: ✓

Appendix B: ArchiMate Elements

Table 8 - ArchiMate motivation elements from [38]**.**

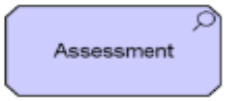
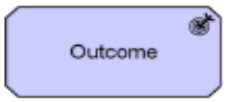
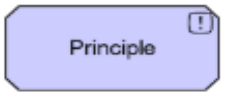
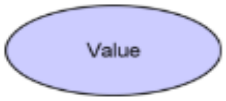
Element	Definition	Notation
Stakeholder	The role of an individual, team, or organization (or classes thereof) that represents their interests in the outcome of the architecture.	
Driver	An external or internal condition that motivates an organization to define its goals and implement the changes necessary to achieve them.	
Assessment	The result of an analysis of the state of affairs of the enterprise with respect to some driver.	
Goal	A high-level statement of intent, direction, or desired end state for an organization and its stakeholders.	
Outcome	An end result that has been achieved.	
Principle	A qualitative statement of intent that should be met by the architecture.	
Requirement	A statement of need that must be met by the architecture.	
Constraint	A factor that prevents or obstructs the realization of goals.	
Meaning	The knowledge or expertise present in, or the interpretation given to, a core element in a particular context.	
Value	The relative worth, utility, or importance of a core element or an outcome.	

Table 9 - ArchiMate business layer from [38]**.**

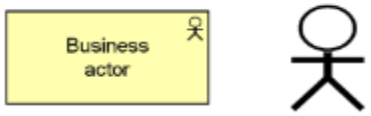
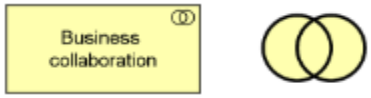
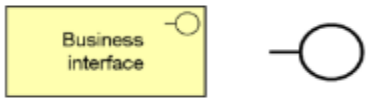
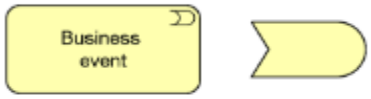
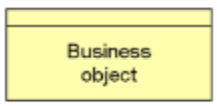
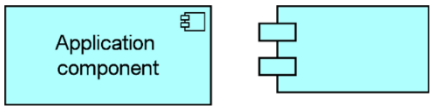
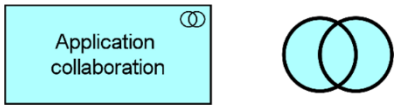
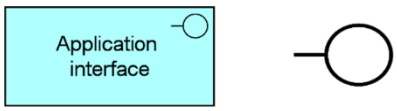
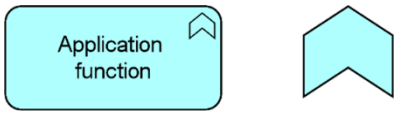
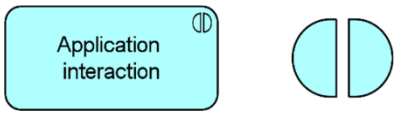
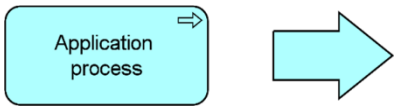
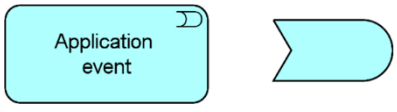
Element	Description	Notation
Business actor	A business entity that is capable of performing behavior.	
Business role	The responsibility for performing specific behavior, to which an actor can be assigned, or the part an actor plays in a particular action or event.	
Business collaboration	An aggregate of two or more business internal active structure elements that work together to perform collective behavior.	
Business interface	A point of access where a business service is made available to the environment.	
Business process	A sequence of business behaviors that achieves a specific outcome such as a defined set of products or business services.	
Business function	A collection of business behavior based on a chosen set of criteria (typically required business resources and/or competences), closely aligned to an organization, but not necessarily explicitly governed by the organization.	
Business interaction	A unit of collective business behavior performed by (a collaboration of) two or more business roles.	
Business event	A business behavior element that denotes an organizational state change. It may originate from and be resolved inside or outside the organization.	
Business service	An explicitly defined exposed business behavior.	
Business object	A concept used within a particular business domain.	

Table 10 - ArchiMate application layer from [38]**.**

Element	Definition	Notation
Application component	An encapsulation of application functionality aligned to implementation structure, which is modular and replaceable. It encapsulates its behaviour and data, exposes services, and makes them available through interfaces.	
Application collaboration	An aggregate of two or more application components that work together to perform collective application behaviour.	
Application interface	A point of access where application services are made available to a user, another application component, or a node.	
Application function	Automated behaviour that can be performed by an application component.	
Application interaction	A unit of collective application behaviour performed by (a collaboration of) two or more application components.	
Application process	A sequence of application behaviours that achieves a specific outcome.	
Application event	An application behaviour element that denotes a state change.	

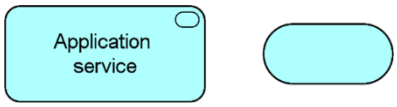
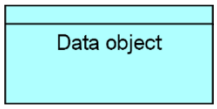
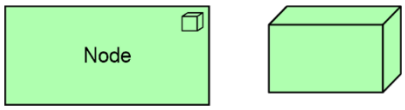
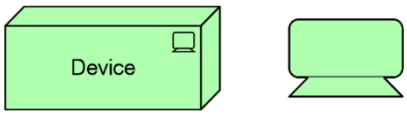
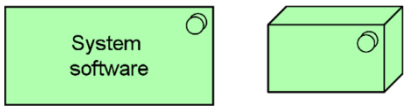
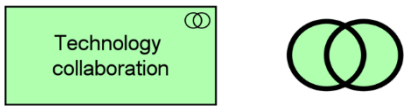
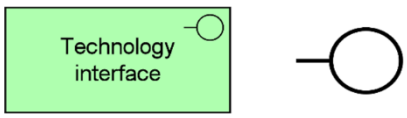
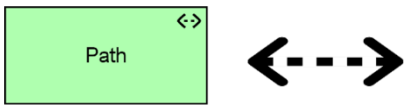
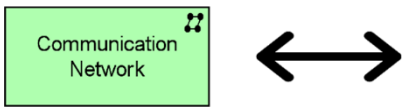
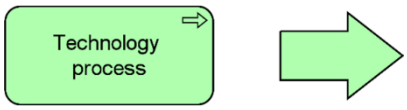
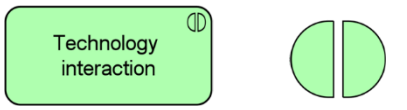
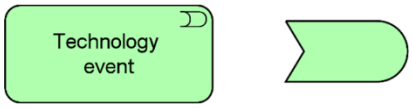
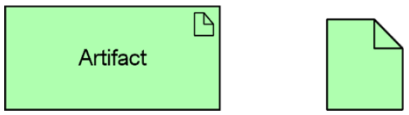
Element	Definition	Notation
Application service	An explicitly defined exposed application behaviour.	
Data object	Data structured for automated processing.	

Table 11 - ArchiMate Technology layer from [38]**.**

Element	Definition	Notation
Node	A computational or physical resource that hosts, manipulates, or interacts with other computational or physical resources.	
Device	A physical IT resource upon which system software and artifacts may be stored or deployed for execution.	
System software	Software that provides or contributes to an environment for storing, executing, and using software or data deployed within it.	
Technology collaboration	An aggregate of two or more nodes that work together to perform collective technology behaviour.	

Element	Definition	Notation
Technology interface	A point of access where technology services offered by a node can be accessed.	
Path	A link between two or more nodes, through which these nodes can exchange data or material.	
Communication network	A set of structures that connects computer systems or other electronic devices for transmission, routing, and reception of data or data-based communications such as voice and video.	
Technology function	A collection of technology behaviour that can be performed by a node.	
Technology process	A sequence of technology behaviours that achieves a specific outcome.	
Technology interaction	A unit of collective technology behaviour performed by (a collaboration of) two or more nodes.	
Technology event	A technology behaviour element that denotes a state change.	

Element	Definition	Notation
Technology service	An explicitly defined exposed technology behaviour.	
Artifact	A piece of data that is used or produced in a software development process, or by deployment and operation of a system.	

Appendix C: Meta model definition using EALang

Schema DBSchema

Schema declares the working schema.

type aggregates, reference, aggregated by, Reference, (*)
type composed of, reference, composes, Reference, (*)
type created by, reference, creates, Reference, (*)
type deleted by, reference, deletes, Reference, (*)
type reported by, reference, reports, Reference, (*)
type located at, reference, locates, Reference, (*)
type owned by, reference, owns, Reference, (*)
type read by, reference, reads, Reference, (*)
type realizes, reference, realized by, Reference, (*)
type updated by, reference, updates, Reference, (*)
type uses, reference, used by, Reference, (*)
type specializes, reference, specialized by, Reference, (*)
type assigned to, reference, assigned from, Reference, (*)
type accesses, reference, accessed by, Reference, (*)
type flow from, reference, flows to, Reference, (*)
type triggered by, reference, triggers, Reference, (*)
type associated with, reference, associated to, Reference, (*)
type influences, reference, influenced by, Reference, (*)

In these lines, the existing relationships are defined (i.e., how can two instances be related to each other).

Note that each relationship needs to have defined an inverse relationship. This implementation is useful for queries. For example, if we consider the relationship “composed of”, it is possible to do a query asking for the components that are composed of A or composed by A. Note also that the “(*)” in the end of each line tell that all classes can use this relationship. It is possible to limit this by enumerating which classes can use it.

class Application Component

property Aggregates, aggregates, listOf, (Application Component)

property Application Components, composed of, listOf, (Application Component)

property Application Layer, text

property Asset Group ID, text

property Availability Value, Double

property Average Value, Double

property Begin Date, DateTime

property Build Cost, Double

property Confidentiality Value, Double

property Critical, Double

property Department, reported by, listOf, (Business Actor)

property Description, text

property End Date, DateTime

property Integrity Value, Double

property IsVersion, Boolean

property Level, text

property Location, located at, listOf, (Location)

property Owned by, owned by, listOf, (Business Actor, Business Role)

property Realizes, realizes, listOf, (Application Service)

property Requirements, text

property Update Date, DateTime

property Uses, uses, listOf, (Application Service, Node, System Software)

property Value, Double

property Versions, realized by, listOf, (Application Component)

The Class keyword defines a Data Type with the respective class name. When a class is declared the following properties, declared in the file, are bound to it, until a new class is defined.

A class has a default Name property that has the same value as the name of the class.

Property declares a property associated with a class. It is possible to use Boolean, DateTime, Double, Text, and defined types as the ones defined above.

When using the defined types, it is necessary to indicate to which other classes is this one related to. For example, the property “Owned by” here represented means that an Application Component may be owned by a business actor or a business role.

class Application Service

property Aggregates, aggregates, listOf, (Application Service)

property Application Services, composed of, listOf, (Application Service)

property Approval Date, DateTime

property Asset Group ID, text

property Availability Value, Double
property Average Value, Double
property Begin Date, DateTime
property Confidentiality Value, Double
property Department, reported by, listOf, (Business Actor)
property Deprecated Date, DateTime
property Description, text
property End Date, DateTime
property External link, URL
property Hourly burden rate (B), Double
property Implemented Date, DateTime
property Integrity Value, Double
property IsVersion, Boolean
property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Actor)
property Predicted number of annual reuse (n), Double
property Production Date, DateTime
property Production investment (Pinv), Double
property Realized by, realized by, listOf, (Application Component)
property Requirements, text
property Specializes, specializes, listOf, (Application Service)
property Total Development Hours (TDH), Double
property Type, text
property Update Date, DateTime
property Used by, used by, listOf, (Application Component, Business Process, Business Actor, Business Role)
property Value, Double
property Versions, realized by, listOf, (Application Service)

class Business Actor
property Aggregates, aggregates, listOf, (Business Actor)
property Asset Group ID, text
property Assigned to, assigned to, listOf, (Business Role)
property Availability Value, Double
property Average Value, Double
property Begin Date, DateTime
property Business Actors, composed of, listOf, (Business Actor)
property Confidentiality Value, Double

property Department, reported by, listOf, (Business Actor)
property Description, text
property End Date, DateTime
property External link, URL
property Integrity Value, Double
property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Actor)
property Requirements, text
property Specializes, specializes, listOf, (Business Actor)
property Type, text
property Update Date, DateTime
property Uses, uses, listOf, (Application Service, Business Service)
property WorksAt, located at, listOf, (Location)

class Business Object
property Asset Group ID, text
property Availability Value, Double
property Average Value, Double
property Confidentiality Value, Double
property Department, reported by, listOf, (Business Actor)
property Description, text
property Integrity Value, Double
property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Role)
property Requirements, text
property Update Date, DateTime
property Value, Double

class Business Process
property Accesses, accesses, listOf, (Business Object)
property Aggregates, aggregates, listOf, (Business Process)
property Asset Group ID, text
property Assigned from, assigned from, listOf, (Application Component, Business Role)
property Availability Value, Double
property Average Value, Double
property Begin Date, DateTime
property Business Processes, composed of, listOf, (Business Process)
property Confidentiality Value, Double

property Department, reported by, listOf, (Business Actor)
property Description, text
property End Date, DateTime
property External link, URL
property Flow from, flow from, listOf, (Business Process)
property Flows to, flows to, listOf, (Business Process)
property Integrity Value, Double
property Is Critical, Boolean
property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Actor)
property Realizes, realizes, listOf, (Business Service)
property Requirements, text
property Specializes, specializes, listOf, (Business Process)
property Specification Document, URL
property Triggered by, triggered by, listOf, (Business Process)
property Triggers, triggers, listOf, (Business Process)
property Update Date, DateTime
property Used by, used by, listOf, (Business Process, Business Actor, Business Role)
property Uses, used by, listOf, (Application Component, Application Service)
property Value, Double

class Business Role
property Aggregates, aggregates, listOf, (Business Role)
property Asset Group ID, text
property Assigned from, assigned from, listOf, (Business Actor)
property Assigned to, assigned to, listOf, (Business Process, Work Package)
property Availability Value, Double
property Average Value, Double
property Begin Date, DateTime
property Business Roles, composed of, listOf, (Business Role)
property Confidentiality Value, Double
property Department, reported by, listOf, (Business Actor)
property Description, text
property End Date, DateTime
property External link, URL
property Integrity Value, Double
property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Actor, Business Role)

property Requirements, text
property Specializes, specializes, listOf, (Business Role)
property Update Date, DateTime
property Uses, uses, listOf, (Application Service)

class Business Service
property Asset Group ID, text
property Availability Value, Double
property Average Value, Double
property Begin Date, DateTime
property Confidentiality Value, Double
property Department, reported by, listOf, (Business Actor)
property Description, text
property End Date, DateTime
property Integrity Value, Double
property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Role)
property Requirements, text
property Update Date, DateTime

class Control Measure
property Associated with, associated with, listOf, (Information Security Risk)
property Begin Date, DateTime
property Control effectiveness, text
property Control Measure ID, text
property Control Owner, owned by, listOf, (Business Role)
property Currency unit, text
property Description, text
property End Date, DateTime
property Estimated Cost, Double
property Identification Date, DateTime
property Implementation conclusion date, DateTime
property Implementation Responsible, assigned to, listOf, (Business Role)
property Implementation State, text
property IsSystemicCorrectiveAction, Boolean
property Realizes, realizes, listOf, (Control Objective)
property Target date for implementation, DateTime
property Realizes Control Objective, realizes, listOf, (Control Objective)

property Realized by, realized by, listOf, (Application Component, Application Service, Business Actor, Business Object, Business Process, Business Role, Business Service, Location, Node, System Software)

class Control Objective

property Begin Date, DateTime

property Control Objective ID, text

property End Date, DateTime

property IsSystemic, Boolean

class Information Security Incident

property Affected department, reported by, listOf, (Business Actor)

property Affects, associated with, listOf, (Application Component, Application Service, Business Actor, Business Object, Business Process, Business Role, Business Service, Location, Node, System Software)

property Associated Corrective Control Measure, associated with, listOf, (Control Measure)

property Associated Corrective Control Objective, associated with, listOf, (Control Objective)

property Associated Risk, associated with, listOf, (Information Security Risk)

property Associated Vulnerability, associated with, listOf, (Vulnerability)

property Availability Impact, Double

property Begin Date, DateTime

property Composed of, composed of, listOf, (Information Security Incident)

property Confidentiality Impact, Double

property Description, text

property End Date, DateTime

property Identification Date, DateTime

property Impact, Double

property Incident ID, text

property Integrity Impact, Double

property IsComponent, Boolean

property Reported by, reported by, listOf, (Business Actor)

property Treatment Date, DateTime

property Triggered by, triggered by, listOf, (Threat Event)

property Verification Date, DateTime

class Information Security Risk

property Asset Group ID, text

property Associated Control Measure, associated with, listOf, (Control Measure)

property Associated Control Objective, associated with, listOf, (Control Objective)
property Associated Loss Event, associated with, listOf, (Loss Event)
property Associated Threat Event, associated with, listOf, (Threat Event)
property Associated Vulnerability, associated with, listOf, (Vulnerability)
property Availability Impact, Double
property Begin Date, DateTime
property Confidentiality Impact, Double
property Consequences, Double
property Description, text
property End Date, DateTime
property Identification Date, DateTime
property Integrity Impact, Double
property IsVersion, Boolean
property Level of Risk, Double
property Likelihood, Double
property Risk ID, text
property Risk Owner, owned by, listOf, (Business Role)
property Selected Option for Risk Treatment, text
property Versions, realized by, listOf, (Information Security Risk)
property Associated Assets, associated with, listOf, (Application Component, Application Service, Business Actor, Business Object, Business Process, Business Role, Business Service, Location, Node, System Software)

class Location
property Aggregates, aggregates, listOf, (Location)
property Asset Group ID, text
property Availability Value, Double
property Average Value, Double
property Confidentiality Value, Double
property Department, reported by, listOf, (Business Actor)
property Description, text
property Integrity Value, Double
property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Role)
property Requirements, text
property Update Date, DateTime
property Value, Double

class Loss Event

property Associated Vulnerability, associated with, listOf, (Vulnerability)

property Triggered by, triggered by, listOf, (Threat Event)

class Node

property Aggregates, aggregates, listOf, (Node, System Software)

property Asset Group ID, text

property Availability Value, Double

property Average Value, Double

property Begin Date, DateTime

property Confidentiality Value, Double

property Department, reported by, listOf, (Business Actor)

property Description, text

property End Date, DateTime

property External link, URL

property Integrity Value, Double

property Location, located at, listOf, (Location)

property Nodes, composed of, listOf, (Node)

property Owned by, owned by, listOf, (Business Actor)

property Requirements, text

property Specializes, specializes, listOf, (Node)

property Update Date, DateTime

property Value, influences, listOf, (Value)

class System Software

property Aggregates, aggregates, listOf, (System Software)

property Asset Group ID, text

property Associated with, associated with, listOf, (Communication Path)

property Availability Value, Double

property Average Value, Double

property Begin Date, DateTime

property Confidentiality Value, Double

property Department, reported by, listOf, (Business Actor)

property Description, text

property End Date, DateTime

property External link, URL

property Integrity Value, Double

property IsVersion, Boolean

property Location, located at, listOf, (Location)
property Owned by, owned by, listOf, (Business Actor)
property Requirements, text
property Specializes, specializes, listOf, (System Software)
property System Softwares, composed of, listOf, (System Software)
property Update Date, DateTime
property Value, influences, listOf, (Value)
property Versions, realized by, listOf, (System Software)

class Threat Event
property Associated Vulnerability, associated with, listOf, (Vulnerability)

class Vulnerability