INCOSE

WESTERN STATES REGIONAL CONFERENCE

# A Formal Approach to Support Complex Security Management

## Case Study of a Moroccan Hospital

INCOSE WSRC · 2025

**AUTHORS**

Anass Rabii, Mohamed Rajraji, and Steven J. Simske

**PUBLICATION DATE**

July, 2026

**SUBMISSION #**

4

INCOSE PUBLICATIONS

# A Formal Approach to Support Complex Security Management: Case Study of a Moroccan Hospital

**Anass Rabii**

**SIWEB, Ecole Mohammadia d'Ingénieurs, BP: 765, Avenue Ibn Sina, Agdal, Rabat, Morocco**
**anassrabii@gmail.com**

**Mohamed Rajraji**

**Walter Scott, Jr. College of Engineering, Colorado State University, 6029 Campus Delivery, Fort Collins, CO, USA**
**Mohamed.rajraji@colostate.edu**

**Steve Simske**

**Walter Scott, Jr. College of Engineering, Colorado State University, 6029 Campus Delivery, Fort Collins, CO, USA**
**steve.simske@colostate.edu**



## Abstract

The criticality of security management stems from the complexity of information systems and the high value of assets and services. The diversity in security management solutions makes organizations responsible for choosing an adequate solution and adapting it to their context. However, the complexity makes the implementation process vary further, complicating choices. Moreover, security management solutions suffer from implementation shortcomings such as lack of guidance or adaptation guides. Grounded in the MBSE paradigm, we made AtlaSec: a methodology supporting security solution implementation and management with security models. This paper presents a case study undertaken to evaluate the security characteristics covered by AtlaSec compared to the needs of a complex system. The case study was done on the information system of a prominent hospital in Morocco with the help of the IT Road consulting firm. This case study also focuses on the impact of formalism on the verification of essential security practices. We found that AtlaSec covers most of the necessary security base practices prescribed by ISO 21827 either through one or many design elements. Using security diagrams that consider the complex nature of links between security concepts creates a cascading effect that shows where actions are required through different facets of security.

## Keywords

AtlaSec, Case study, HIS, Security, ISO 21827.

# Introduction

The digitalization effort expended by organizations looking to capitalize on improvement opportunities introduces a higher level of complexity into their information systems and as a result, their security shifts to the broader paradigm of systems engineering. This complexity means that the secured information system is similar to a chain, where usually organizations focus on the improvement of technology and human resource training. This explains why some cyber-attacks not only target the gaps in the architecture or flaws within the software, but also target non-IT staff or resort to social engineering (Verizon Business, 2021). Additionally, the inclusion of critical assets such as client personal data,

medical equipment or government intelligence makes security engineering a critical aspect to consider. Consequently, corporations, governmental entities and security experts banded together to create security solutions such as hardware solutions, software solutions, standards, best practices and legislation to reduce security risks. This gives organizations access to a plethora of solutions to implement and adapt to their context depending on their size, budget, field, staff, etc. Beforehand, the security officer uses the recommendations of security standards as well as legal and contractual obligations as the basis to elaborate the security policy. Prominent examples of such references include the security standards ISO 21827 (ISO, 2008) and ISO 27000 (ISO/IEC, 2013; ISO, 2013)(ISO/IEC, 2018) family, the NIST cyber security framework (National Institute of Standards and Technology, 2018), the NERC critical infrastructure protection standard (North American Electric Reliability Corporation, 2015), governmental security frameworks(DGSSI, 2013; White, 2011) ref and security maturity models (Yulianto, Lim, & Soewito, 2016) (Luis Enrique Sánchez, Daniel Villafranca, 2007). However, these solutions establish how security should be managed either to reach a defined goal like certification or for continuous improvement. However, organizations are still liable for the adaptation effort required for implementation.

The high variability introduced during implementation and adaptation makes any security policy or security management solution's effectiveness difficult to ascertain during realization. Moreover, these standards can be challenging to implement regardless of resources available. In fact, Javaid et al. (Javaid & Iqbal, 2017) suggest that the existing security standards favor larger scale organization to the detriment of small & medium enterprises while also being too generic or too specific to certain contexts making implementation paths unclear. However, large corporations as well as governmental entities face similar issues where their security maturity is still low (Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, 2015). Mubarak et al. (Mubarak, S.; Heyasat, H.; Wibowo, 2019) suggest that such security standards and solutions are necessary but they require support during implementation. Moreover, our systematic literature review on security maturity models (Rabii, Assoul, Ouazzani Touhami, & Roudies, 2020) highlights that academia opts for the production of domain specific security maturity models to facilitate implementation. This joins the trend of existing research to produce more lightweight solutions based on existing security standards for ease of use (Ponsard, Massonet, Grandclaudon, & Point, 2020; Teufel, Teufel, Aldabbas, & Nguyen, 2020). This further emphasizes the importance of addressing complexity in security for better implementation.

Historically, when complexity arose in software engineering, modeling software composition and behavior was the customary way to analyze and produce complex products. Similarly, fields such as electrical engineering, mechanical engineering, and even architecture rely on Computer Aided Design (CAD) software to produce complex artifacts. In fact, the driving principle in the paradigm of Model Based Systems Engineering (MBSE) is the use of models as a cornerstone for requirement specification, analysis, design, implementation and verification of a complex concept. Models simplify these concepts through a formal representation that complies with semantic and syntax rules. Models should be used to spark discussion about the phenomenon while leaving a traceable trail of improvements. Thus, the formalism allows increasing quality, identifying risks, detecting flaws, and rectifying flaws before implementation, which leads to reduced costs. It also allows the execution of tests and the verification that the requirements are satisfied as early as the design phase (Moody, 2009).

In line with the MBSE paradigm, we developed the AtlaSec method to formalize and guide the implementation of security processes in complex contexts. AtlaSec formalizes the security characteristics of a complex system through a SysML-based security Domain Specific Modeling Language (DSML). This method offers a set of security diagrams to model, analyze and verify security characteristics of complex systems. We also provide a cyclical procedure to support the usage of the security diagrams

to insure continuous improvement. The procedure addresses security planning, implementation, and verification using OCL verification queries on the modeled security characteristics. Initially, we put portions of AtlaSec's security DSML to practice on HIS and security breach case studies to study security requirement elicitation, task monitoring, and operational responsibility management (Rabii, Assoul, & Roudies, 2020) (Assoul, Rabii, & Roudiès, 2021). This has allowed us to verify the usability of the AtlaSec method on individual security aspects and improve them. To further ascertain the applicability and contribution of the AtlaSec method, we applied it to the Hospital Information System of a specialty hospital in Rabat, Morocco. The aim of the HIS case study presented in this paper is twofold: to experiment the AtlaSec method on the ground on a chosen hospital's information system and to show the importance of a holistic and formal approach in dealing with complexity while ensuring the security of this HIS. The originality of this paper is predicated on both the pragmatic approach of the case study method as well as the choice of Hospital Information Systems. In fact, HIS are systems of systems (SoS) that contain heterogeneous components, comprise a high number of interconnections, and fulfill the conditions of: scalability, functional and organization autonomy, physical distribution and a centralized command center. Furthermore, HIS are complex organizations with critical security requirements. Their duty to continuously provide adequate care to patients requires insuring the availability and integrity of their data and processes. Moreover, they are subjected to various legislative obligations for having to insure patient personal data confidentiality as well as various technical and medical requirements.

On one hand, we undertook this study in response to the gaps identified in the implementation of security standards, academic maturity models as well as feedback on the causes of security breaches. Firstly, our Systematic Literature Review (Rabii, Assoul, Ouazzani Touhami, et al., 2020) highlights a gap within academia in terms of analyzing the implementation of security management solutions. The studies that have analyzed these implementations express overall positive results that require further research to consolidate. Thus, this case study aims to highlight the contribution of a holistic formal approach for distinguishing the impact of security solutions and by extending their validation. Secondly, this case study comes as corollary following previous case studies analyzing security breaches that have occurred within organizations that highlight issues in the implementation of the security policy. For example, we consider the case of the Capital One data breach (Novaes Neto, Madnick, Moraes G. de Paula, & Malara Borges, 2020), an interesting in-depth analysis of the shortcomings in policy implementation. In this example, Capital One's avant-garde policy included its involvement in security standard refinement and being at the forefront of the technological improvements of its system. However, this case can be considered a typical study that showcases that organizations can fully grasp which security controls their security policy requires but still display a gap in their implementation, thus causing breaches. As it is highlighted in the Capital One discussion and our previous analysis (Assoul et al., 2021), the influence of intertwined components has an effect on the overall state of security (managerial problems leading to neglected tasks). Hence, we believe that complexity of the context needs to be addressed to study security.

On the other hand, we initially studied different security standards (Anass, Saliha, & Ounsa, 2020), governmental frameworks (Anass, Saliha, Khadija, & Ounsa, 2019) and security management solutions to assess their effectiveness and identify the reasons behind the production of solutions that, seemingly, are similar to the existing standards. Our research then shifted to tackle the complexity at the heart of the implementation issue through the formalism brought forth with models. To this end, we have elaborated the AtlaSec method that proposes the use of security-oriented diagrams to analyze and improve the design of security policies. These model-based representations offer a dynamic and readily updatable representation, unlike static text-based policies. The ability to update these diagrams easily ensures that the security policy can evolve

rapidly in response to changes within the system, emerging threats and changes in the technological and governance landscape. Moreover, their comprehensive nature provides a holistic view of the security of the system, in line with the systems engineering principle of holism,allowing for a more integrated and thorough assessment. Thus, the first objective of this study is to ascertain the necessary security characteristics that should make up the AtlaSec security diagrams. The second objective of this case study is to assess the utility of this representation of the security aspects that characterize a HIS as a representative complex system, along with the formal assessment of security management it provides. In this paper we evaluate the capacity of AtlaSec's security modeling language to encompass the security engineering process. Then, we evaluate AtlaSec's contribution to the design and verification of the security policy. However, this study will neither attempt to identify the optimal security management solutions nor assert how security should be managed.

In the following section, we will discuss this Case Study's methodology and design. In section 3, we provide an overview of AtlaSec, the security DSML and the security concepts it models. In section 4, we will present our analysis of the data and the lessons learned from it. Finally, section 7 will conclude with study implications and future works.

# Design of the case study

## Rationale & Objectives

The rationale behind this study is to bridge the gap between the design of security management solutions and its implementation. Security officers have access to a plethora of security standards and frameworks to adapt into the context of their organizations. However, most of the prominent standards lack implementation paths and require guides. This is why we see an increase in lightweight solutions that are based on the existing standards. Their objective is to reduce the level of complexity through specialization. The specialization can be to either a domain or an aspect of security. Security breaches at organizations that grasp which standards, policies, and/or controls to administer further demonstrate that the core issue is implementation. Our rationale is to face the complexity at the source of the implementation issue rather than missing the depth provided by the standards. We began by studying existing security management solutions and evaluating their mainspring and effectiveness, which exhibited the implementation issues. We proposed the AtlaSec method comprising security diagrams and implementation paths to deal with complexity. This study comes at the validation phase of our proposed method using the case study methodology. The methodology can be used to answer how or why questions and to study phenomena that cannot be dissociated from their contexts. In fact, our objective is to determine what the required concepts are to formalize the design of security management solutions and how such a formalism can facilitate dealing with complexity. Moreover, the context of Systems of Systems is the source of the complexity and its security cannot be dissociated from it.

In the inception of this study, we considered many choices of complex systems such as electrical grids and smart cities. However, through the research team's contact network, we identified an ongoing IT auditing mission led by the company ITRoad (Road, n.d.) with the goal of improving the smart hospital's maturity and determining its improvement paths. ITRoad has agreed to provide the anonymized data to support the case study we were building. Later, ITRoad provided further data coming from nine more hospitals abroad to enrich the study. This is when the qualitative data collected reached a critical mass post-triangulation to push the case study project to fruition. Since the earliest stages, we framed the case study as an Embedded Case Study since Hospital Information Systems include a variety of units that are considered systems such as the radiotherapy unit, the anesthesiology unit, the pharmaceutical unit, and the surgical unit. The case will focus on a select set of services since the rich composition of each service makes the amount of detail quickly become unmanageable.

## Theoretical framework

Our theoretical framework is based on the existing ISO security standards ISO 21827 and the ISO 27000 family. According to ISO, security engineering as a practice includes three basic areas: risk management, artefact management, and insurance provision. First, the risk dimension deals with identifying threats and vulnerabilities that might endanger the system. On top of these two concepts, the framework includes risk factors such as threat agents, impacts, and incidents. Second, the artefact engineering area relates to other engineering disciplines that create and implement solutions to deal with security risks. Thus, the framework includes concepts relating to a typology of artefacts and their roles. Third, the insurance provides the confidence that the security solutions implemented reach their defined goals, satisfy business needs, meet the security requirements and reduce the security risks. The framework includes concepts such as risk reduction and requirement satisfaction for the attainment of security goals. Initially, we extracted these concepts from a comparative analysis between prominent security management solutions (Anass et al., 2020). Then, we consolidated them with findings from preliminary research done with the help of engineering students and HIS experts.

## Research Questions

First, we want to identify what the specific security characteristics and needs of the HIS are (Research Question 1). This research question is for compiling the security information required, according to AtlaSec's framework, to analyze the security state of our HIS. This is divided into three aspects: system composition, risk factors, and insurance requirements. This approach exposes the relationships between the components of system, allowing their valuation in accordance with their importance to the HIS as a whole but also with their so-called CIA (Confidentiality, Integiry, and Availability) amongst other variables. Secondly, we ascertain the variables involved in risk assessment. This allows one to properly address risk sources in the proper priority order through the adequate security controls. As a consequence, the insurance in the security of the HIS means a conviction that the security goals and needs, represented as requirements, are satisfied. The next question relates to the methodology's usage for formal representation and assessment of the management of the HIS security (Research Question 2). The AtlaSec methodology aims to facilitate the verification of the essential security practices within a security engineering approach. This enables the verification of the validity of security policies through design testing. Moreover, this simplifies the daily verification, allowing the HIS to substantiate its insurance at all times. The research questions formulated are the following:

RQ1: What are the security characteristics and needs of the HIS?

RQ 1.1: What are the components to consider for the HIS security management?

RQ 1.2: What are the risk factors to consider for the HIS security management?

RQ 1.3: What are the required processes to insure the security of the HIS?

RQ 2: How does the formalism support the verification of the essential security practices of the HIS?

## Planning

### Method data collection

The main source of information for the case study is a set of technical audit workshops as well as preemptively collected internal documentation. ITRoad follows a controlled and documented IT audit process compliant with auditing standard ISO 19011. The certified process shown in Fig 1 guarantees the quality of the collected data. The overall mission took place starting November 2020 until April 2021. During the initial contact, the HIS' management and ITRoad set out to assess the information system's maturity as well as define and then act out a strategy for its evolution. In the preparation phase, internal documents were accessed and a

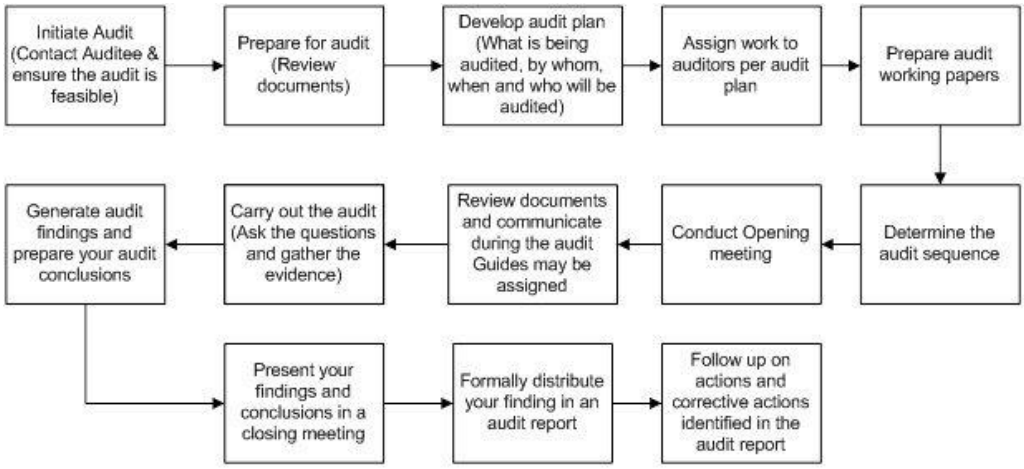


**Fig1: ISO 19011 IT auditing process**

questionnaire survey was distributed to collect information from different actors within the IS. The internal documentation collected presents the internal IT roadmap of the hospital, a census of the infrastructure components, and the documented processes. The involved hospital stakeholders include the Chief Information Officer, IT support, infrastructure and security managers and their administrators. The IT auditors then consolidate information about the infrastructure, the logical and network architectures, the security and the asset exploitation policies. After that, the data is aggregated into workshop reports, security charters, technical and security risk maps, and process handbooks. The hospital CIO and IT managers validated each deliverable. The overall mission hinges on data collected from employees from different management levels (observer triangulation), internal documentation, and auditor observation and analysis made over several months (source triangulation). Moreover, the data collected was weighed against results from overseas partners. This helps identify gaps in the required data during collection. For our case study, we included secondary data from research into HIS architecture composition, process, security risks and requirements.

## Method data selection

First, we filtered the data based on the security framework we devised: system artefacts, risk factors and security requirements, needs, and goals. In the beginning, we scoured the documents regarding the security policy and the roadmap to identify the goals, needs and obligations of the HIS. We completed this list with the legal requirements defined by the Moroccan government for both security and medical related issues. Since requirements are an integral model element for system engineering, we translated each of these elements into requirements with a priority level. This gives us our initial input for the security requirement diagrams. Next, we sorted the system components into the different types of assets followed by determing which unit they belong to. We consolidated this data with academic data related to HIS composition. Then, we studied the documents detailing each business process to identify which assets collaborate with each other and which actors are required to execute the tasks. We consolidated this data with standardized HIS process mapping from ANAP (Jabbar, Lahboube, Souissi, & Roudies, 2017). Next, we determined which actor within the system is the responsible for each asset and task. This is our initial input for the system composition diagram. Lastly, we extracted the risk factors for each system from the risk map. Then, we completed it with information about typical vulnerabilities, threats that exist in HIS. This is our initial input for the risk analysis diagram. Iteratively, these data pools were completed after each cycle of data collection and analysis. During each iteration of scenario testing, we improved the model by adding new concepts, removing them, or splitting a concept into many.

### Method data analysis

In order to analyze the attainment of our objective of providing a supporting solution for security management, we need to identify the practices of security management, extract their goals, and assess whether AtlaSec helps meet them. The ISO systems security engineering capability maturity model (ISO, 2008) (ISO 21827, Table 1) defines a set of 11 security process areas that encapsulate the essential aspects of security engineering. Each of these process areas has goals that can be met through the implementation of each essential base practice. Therefore, our analysis will comprise evaluating whether AtlaSec formalizes the characteristics necessary for each base practice as well as cover all the security practices within its procedure and support their realization. The following table assembles the ISO security process areas and their goals required. We ordered them alphabetically, as they are ordered in the standard, to dissuade prioritization or spreading them over different lifecycle phases.

**Table 1: List of ISO 21827 security process areas and their goals**

| Process Area | Goal |
|---|---|
| PA01: Administer Security Controls | Security controls are properly configured and used. |
| PA02 Assess Impact | The security impacts of risks to the system are identified and characterized. |
| PA03 Assess Security Risk | An understanding of the security risk associated with operating the system within a defined environment is achieved;<br><br>Risks are prioritized according to a defined methodology. |
| PA04 Assess Threat | Threats to the security of the system are identified and characterized. |
| PA05 Assess Vulnerability | An understanding of system security vulnerabilities within a defined environment is achieved |
| PA06 Build Assurance Argument | The work products and processes clearly provide the evidence that the customer's security needs have been met |
| PA07 Coordinate Security | All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions;<br><br>Decisions and recommendations related to security are communicated and coordinated. |
| PA08 Monitor Security Posture | Both internal and external security related events are detected and tracked;<br><br>Incidents are responded to in accordance with policy; and<br><br>Changes to the operational security posture are identified and handled in accordance with the security objectives. |
| PA09 Provide Security Input | All system issues are reviewed for security implications and are resolved in accordance with security goals;<br><br>All members of the project team have an understanding of security so they can perform their functions;<br><br>The solution reflects the security input provided. |
| PA 10 Specify Security Needs | A common understanding of security needs is reached between all parties, including the customer |
| PA 11 Verify and Validate Security | Solutions meet security requirements;<br><br>Solutions meet the customer's operational security needs |

**Table 1: List of ISO 21827 security process areas and their goals**

In the results section we will go over the goals of each process area and detail how they are achieved providing detailing from the HIS case study.

# AtlaSec Overview

We put forward the AtlaSec method to support the management of information security management

systems (ISMS) in complex contexts. AtlaSec aims to guarantee the rigor of the designed security measures with the consideration of security throughout the entire engineering lifecycle. We created AtlaSec according the research methodology of Design Science (Fuller, 1957) where the aim is to produce artefacts (concepts, models, methods or instances) to resolve persistent issues. To this effect, AtlaSec ascribes to the systems engineering paradigm and is based on the MBSE approach. However, we need to dispel the misunderstanding around graphical models. The formalism of graphical modeling is in fact capable of generating serious analysis (Bertin, 1987)(Harel & Rumpe, 2004). The development that occurred around models in the field of Model Driven Engineering showcases the possibilities that come from the maturation of the field.

Four principles have guided the design of AtlaSec. At its foundation, AtlaSec is positioned at different levels of abstraction to address the complexity issue with a scalable vision. The first driving principle is the adaptability to complex systems. The heterogeneous nature of the components and their interoperability complicates the definition, implementation, the monitoring and even the alteration of the security policy. This is why AtlaSec addresses in detail the system composition, emphasizing on the collaborations between assets and the responsibilities of its actors. The second driving principle is the adaptability to the context, wherein the solution must provide a level of freedom in regards to the domain, the size of the organization, and their choices of security policy. The genericity insures that AtlaSec is applicable to all contexts. The third driving principle is modularity to guarantee evolution of technology or in security techniques. AtlaSec insures an iterative and progressive implementation of security controls to improve the performance of the ISMS. Moreover, the insurance produced by the security systems is not permanent; AtlaSec needs to address timely changes for supervision purposes. Lastly, we align with the Design Science methodology where the last principle is security standard centricity. They are an important and holistic resource in the base of knowledge and cannot be disregarded.

In order to support our approach, our defined framework is based on the three aspects of security engineering defined by ISO 27000: artefact engineering, risk management and insurance production. Securing a system boils down to implementing the adequate artefacts to reduce the security risks and fulfill the security needs and requirements. As long as these artefacts are functional, they confer insurance in the ISMS. However, we introduced a distinction to emphasize the importance of processes. Consequently, we organized our solution into four dimensions including each one of these aspects: system composition (artefacts engineering), risk analysis, security requirement management, and process management. AtlaSec relies on a security oriented DSML and a procedure to guide its implementation. The DSML is based on a set of security concepts for each dimension of the framework. These concepts are a result of a comparative study amongst prominent security management solutions from academia, the industry, and e-Gov(Anass et al., 2020). Next, we have chosen to rely on the standards in system engineering modeling SysML to create our security diagrams. The SysML requirements diagram, block diagrams, and activity diagram align with our driving principles of genericity and modularity. We created our security diagrams through the definition of a graphical syntax using the SysML extension mechanism: profiling. Thus, we created a security modeling language consisting of four profile packages for each aspect of the framework. In order to complete these profiles, we defined a set of constraints using the Object Constraint Language. OCL allows us to append restrictions that cannot be modeled on each model element as well as act as a query language for verification. Next, we created an implementation procedure for their use following the Deming wheel and the primordial processes prescribed by the ISO security standards. The AtlaSec cyclical procedure is a hybrid top-down and bottom-up approach where the decisions and objectives are set by top management then are implemented by managers but also implementation results influence future iterations. Naturally, it requires the participation of actors from all hierarchical levels (Asset Managers, Risk

Managers, CISO, and System Owner). The next sections detail the components of each package.

## System Composition Package

We consider that organizations are composed of systems that interact with one another, containing assets that also interact to attain a defined goal. Thus, the package contains the stereotypes "System" and the "Assets" that compose them. Systems possess a logic similar to that of set theory where an asset can belong to one or many systems. An inherently autonomous asset can be represented as a system. The systems do not change when their composition changes but rather when their purpose changes. This also means that the importance of an asset depends on the role it plays for each system. Assets can be specialized into primordial assets (information and processes) or support assets such as "hardware", "software", "site", or "human resource". This allows us to model different properties for each type such as distinctly associating responsibilities or tasks to the "human resource" stereotype. Every primordial asset is supported by one or many support assets. This allows us to trace critical areas where any critical asset should be protected along with the components that directly interact with it. Lastly, we also model tasks as the realization of a "Process" that can be assigned to human resources.

## Process package

For security management, we must consider security processes and business processes alike. The stereotype "Process" behaves like the model element "Activity" and as a system component. This allows us to also detail them in activity diagrams. We dedicated a standalone package for processes to assign to them specific characteristics such as the stereotypes "Performance Indicator", "Guidance", "Goal," and even "Quality Requirement". The quality requirements are design elements that have to be satisfied by the processes themselves and can be verified by "Quality Assessment Mechanisms". We use the predefined associations "satisfy" and "verify" but we extended them to include properties relating to the time of execution. This is necessary since these operations do not yield permanent results meaning they should be periodic. During the creation of these profiles, we realized that the concept "requirement", by definition, is applicable to the entire system not to a specific model element. We wanted to restrain this scope through the definition of the association "affects" where only processes are affected by the quality requirements defined. We included in this association the property "scope" that allows us to extend the range of effect of the requirement for example to adjacent model elements.

## Risk analysis package

The objective of this package is to gather all risk factors and variables required for risk analysis for each asset. By definition, each asset has "vulnerabilities" that can be exploited by "threats" emanating from "threat agents". However, the ISO standard defines the concept of exposure to refer to the association between threat, vulnerability and impact that is considered the source of harm. In fact, the exploitation of a vulnerability might affect other assets. Therefore, we included the concept resulting from the association of threats and vulnerabilities: "incident scenarios". It is by studying the "impact" of incident scenarios on assets that we can obtain the concept of "risk". Each incident scenario can be realized and catalogued as an "incident". Thus, this package includes concepts that are the result of concept pairings. In UML, these pairings are modeled through association classes, a model element that is both an association and a class. Therefore the pairings {(threat, vulnerability) = incident scenario} and {(incident scenario, asset) = impact} are modeled as association blocks. This could be replaced by the creation of a model element "exposure" as it is defined by the triplet, but modeling IDEs usually do not support n-tuple associations. Lastly, we include the model element "security control" as the assets designed to reduce the risks to the acceptable level and protect assets.

## Security Requirement package

The central concept in this package is "Security requirement". These are the conditions the system or specific assets must verify for the attainment of the

organization's goals and satisfy its needs. SysML includes a rich set of associations to model requirement satisfaction and verification. We extended these concepts to include temporal properties for testing purposes but we have kept the same semantics. Thus, security requirements are satisfied by security controls and are verified by "security evaluation mechanisms". Similarly to the process package, we added the association "affects" to designate which system or asset is affected since security requirements do not necessarily apply to the entire system. We also created subtypes of security requirements depending on their sources: internal requirement, contractual requirement, domain requirement and legal requirement. This differentiation between sources allows us to prioritize differently depending on the source (legal text, customer needs) and to remove requirements at the end of a contract or group a standards' requirements for audits. It also allows us to handle conflicts between different sources.

# Report and Dissemination

The objective of this case study was to evaluate the impact of a formal and holistic approach on an on the field HIS. To this end, we identified the process areas that encapsulate the essential practice of security engineering and their goals from the ISO 21827 standard. Therefore, we will begin with assessing the security characteristics modeled by AtlaSec. We verify whether the models encompass each process area's set of prescribed practices (Research Question 1). For each process area treated, the diagrams will only display the design elements and properties relevant to the requirement to not overcrowd the diagrams. Then we assess how these modeled concepts can aid the HIS in the production of insurance in the ISMS (Research Question 2). For more readability, the process areas will be addressed according to their content. The security diagrams modeled below were all created and tested on the Eclipse Modeling IDE. We adapted the IDE to model our SysML security profile.

### Specify security needs

We will begin with Process Area 10 from ISO 21827 as it will help us set the context of the studied case units. The purpose of this process area is to explicit the needs related to the security of the system emanating from different parties.

Gain understanding of the customer's security needs: The first party is the system itself. The primary mission of each system affects security considerations since it must remain operational (Base Practice 10.03). Therefore, we must understand the purpose of the analyzed system. In this paper, we study two case units within the hospital: the oncology unit and the pharmacy unit. Thus, we start with detailing the mission of these two units. This understanding of their activities helps better determine the security context.

The oncology unit consists of two sub-units: the hospitalization unit and the day hospital unit. Both units carry out similar missions but for different patients. The hospitalization unit cares for patients that require a long chemotherapy protocol with hydration portioned over multiple days. The day hospital, in comparison, provides the same services but for patients who do not require to stay more than 12 hours. The day hospital is the main service of the hospital as it receives up to a hundred patients daily. The processes for each unit are represented in the process diagrams below. As an example, we detail the "oncology consultation" process by providing some of its characteristics.

The pharmacy unit handles the management, preparation and distribution of medication to the hospital patients. It is composed of four sub-units:

- Storage management unit: first, this unit handles the supply of pharmaceuticals (cytotoxic, non-cytotoxic) and medical devices as well as storage areas. This unit also handles orders of such items for the hospital. Second, it manages the stock of products data. Lastly, it manages delivery and distribution services for hospitals units.
- Sterilization unit: Its mission is to manage and track the sterilization of all medical equipment.

- Pharmacovigilance unit: its mission is to evaluate and keep track of side effects of all used pharmaceuticals in the hospital.
- Cytotoxin preparation unit (CPU): this unit possesses its own storage unit for critical cytotoxins that it manages. It also manages chemotherapy prescriptions. The CPU validates pharmaceutical orders and provisions of medication. Lastly, it handles the necessary preparations to distribute medication.

Likewise, the processes for each unit are modeled in the process diagram below (Fig. 3). The utility of these models, for this Process Area, is to ascertain the security needs that emanate from the business processes of the HIS. Inputs and outputs display the link between assets and the process itself. This is necessary since from a security perspective we need to know which assets are required for the realization of the process (example: Patient medical history). In order to comprehensively model each business process, we also specify its goals and performance indicators. Goals describe the desired result of the process in question. Performance indicators are the concrete aspects to measure to ascertain if the process realization is nearing desired results. Lastly, quality requirements are an essential aspect for the security standard. They distinguish an effective process from a basic or flawed version of it. In our example, creating a space for discussion with newly hired medical staff about cases is an established training by seeing practice. Thus, in its implementation, the satisfaction of the quality

requirement distinguishes a process from another making it necessary to model.

<u>Capture security view of system operation:</u> The next step to understanding the security context of each HIS unit is to capture their composition from a high-level security-oriented view (Base Practice 10.04). This view should include, amongst other concepts, roles, responsibilities, assets, information flow, and resources. The system composition diagram below (Fig. 4) highlights all these aspects for the oncology unit. In this composition view, we see which primordial and support assets are involved in the implementation of the previously modeled business process "oncology consultation". In this example, the clinical oncologist needs to gain access to existing patient medical data through the management solution Mosaiq on the hospital computer. Mosaiq is a

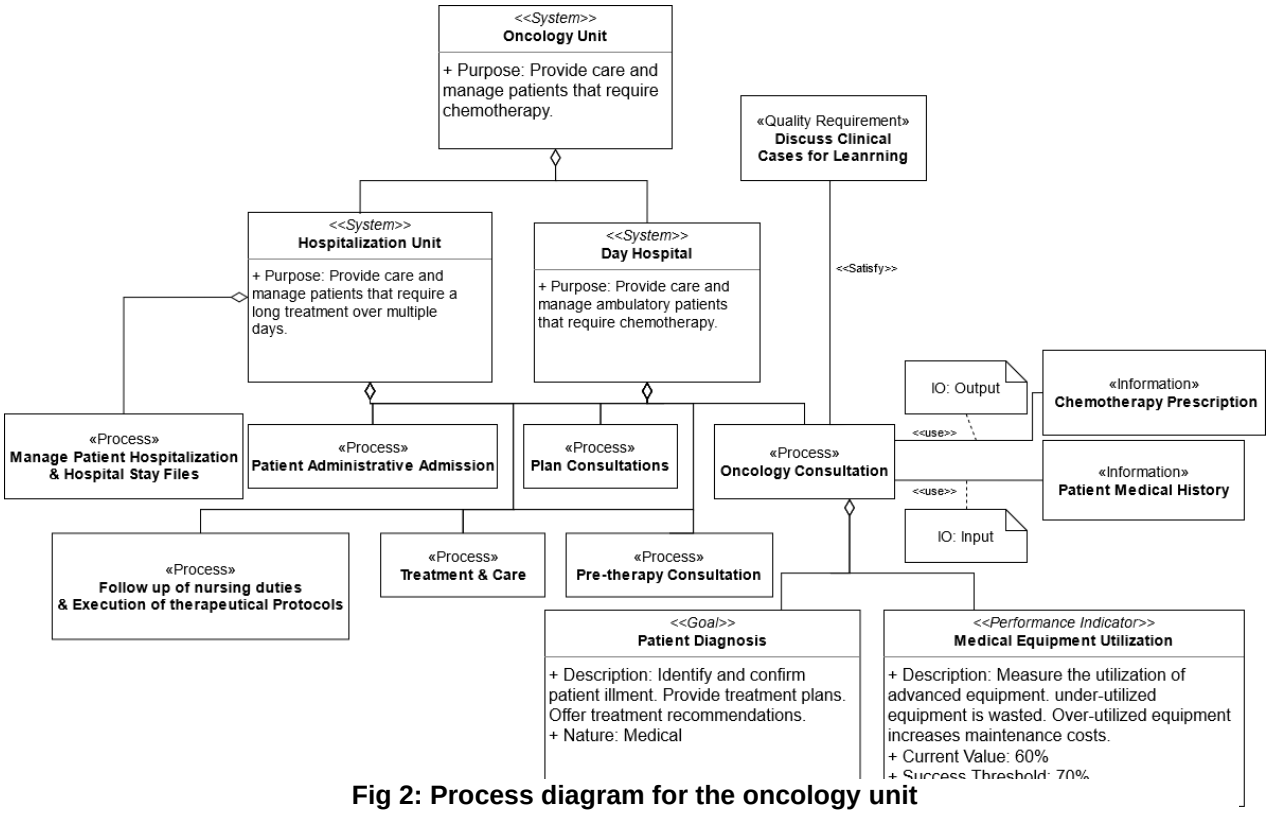


**Fig 2: Process diagram for the oncology unit**

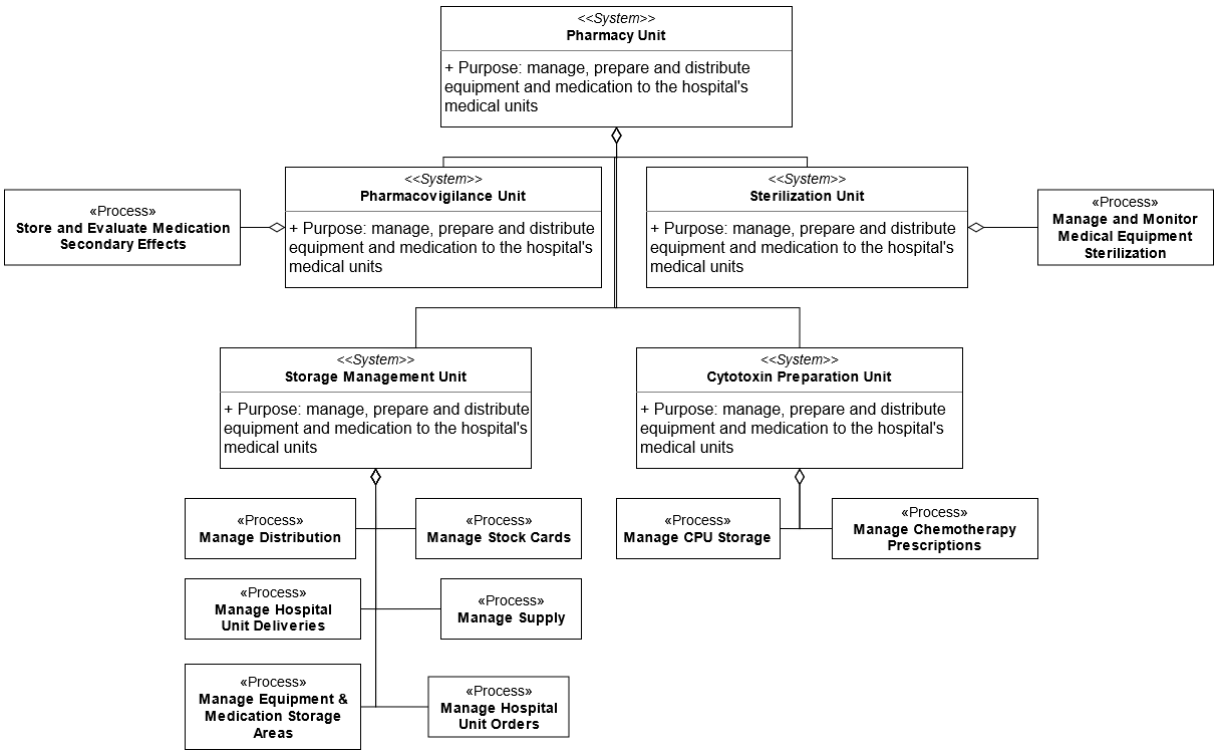


**Fig 3: Process Diagram for pharmacy unit**

software solution that manages patient charting, imaging, prescriptions, and oncology analytics covering the entire oncology chart. Thus, Mosaiq interfaces with the other patient data management solutions to consult and update any patient medical data. Mosaiq provides the necessary data for the consultation and suggests treatments. Then, the doctor uses the MRI scanner for the periodic clinical assessment. The data collected by the scanner is stored and is used to determine the adequate prescription. The prescription is later used as an input to determine the details of the chemotherapy sessions. Thus, this model provides design elements for all the required concepts by the ISO 21827 standard. This model concretizes the implication that securing processes is equivalent to securing the assets that support them. For example, securing the process "oncology consultation" is equivalent to securing the assets "Patient Medical Information", "Mosaiq","MRI Scanner" and the assets they interact with. However, each asset's contribution is different in importance to the realization of the process hence why they have different valuations. Moreover, models visualize the information involved in each process and the support assets it will interact with in its lifecycle. For example, we see that patient medical data is stored in the database, utilized by Mosaiq, transported in the network, and then displayed or edited on the doctor's computer. The model also includes each asset's value. This valuation is calculated based on a formula that considers factors such as confidentiality, integrity, availability, reliability and cost. Since data is a primordial asset, the model highlights its supporting assets that should be protected to protect the data itself. Thus, the value of these support assets rises since they support critical information. We can also see the roles of actors through responsibilities and tasks. Each task is a realization of a process by an actor. For example, it is the doctor's duty to supplement the results of the MRI scan and its interpretation on the Mosaiq platform. Furthermore, the models show which actors are responsible for managing certain asset aspects. The model highlights differences in responsibilities: the doctor is responsible for the usage of the MRI scanner and the infrastructure engineer is responsible for the security of the network.

<u>Capture High-level security goals:</u> Now that the purpose and composition have been fleshed out, we can capture the high-level security goals (Base Practice 10.05). However, the security goals are not

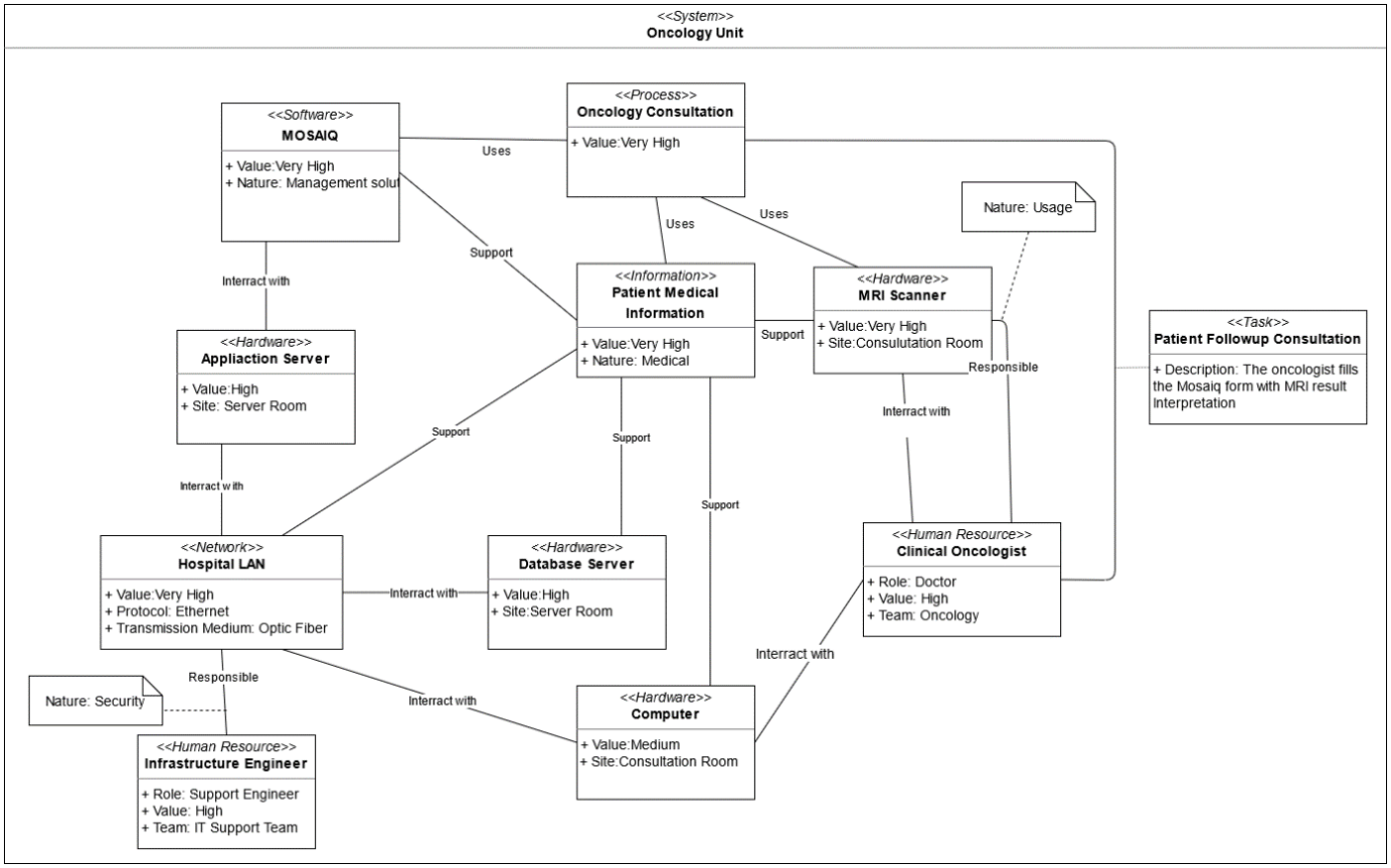


**Fig 4: System composition diagram for the oncology unit**

unique to units but instead are applicable to the entire HIS. These are the high security objectives that are captured in the security policy. The security policy contains sections for the overall state of security of the hospital, data privacy, asset usage, access control, monitoring, training and third party involvement. Explicitly, the hospital security policy dictates that access to assets must be given preemptively and should be periodically updated. Actors are forbidden to use assets for purposes outside the scope of their tasks. Mobile devices must always be password protected and must never leave the premises. Communication via email should be limited where possible, especially externally, and should solely use professional email addresses. Lastly, all employees undergo training to a level appropriate for their tasks and for the improvement of the hospital. Furthermore, the hospital implements all the appropriate mechanisms to safeguard its assets.

However, these sections are not exhaustive. The policy incorporates laws the HIS must abide by (Base Practice 10.02) standards it aims to implement (Base Practice 10.02) and the customer needs that constrain it (Base Practice 10.01). These areas must be considered in tandem to produce a holistic security policy. Firstly, the policy defines what the minimal security level of its HIS should be and which standard it uses as a reference. In this hospital, the HIS should be at least ISO 27001 certified. An external auditing firm periodically verifies the validity of this certification. Secondly, the hospital must satisfy the national regulation. Morocco has passed the 09-08 legislation on the protection of personal data in 2009. This legal text specifies the data owner's rights such as to be informed during data collection, to access their data, to alter their data or ask for deletion. Moreover, the hospital falls under the category of vital organisms and must implement the national directives for the information system security (DNSSI). However, the DNSSI is based on ISO 27001, meaning that being certified makes the hospital compliant with the DNSSI. Thirdly, the customers for our case units are patients and pharmaceutical providers. Thus, the security needs correspond to

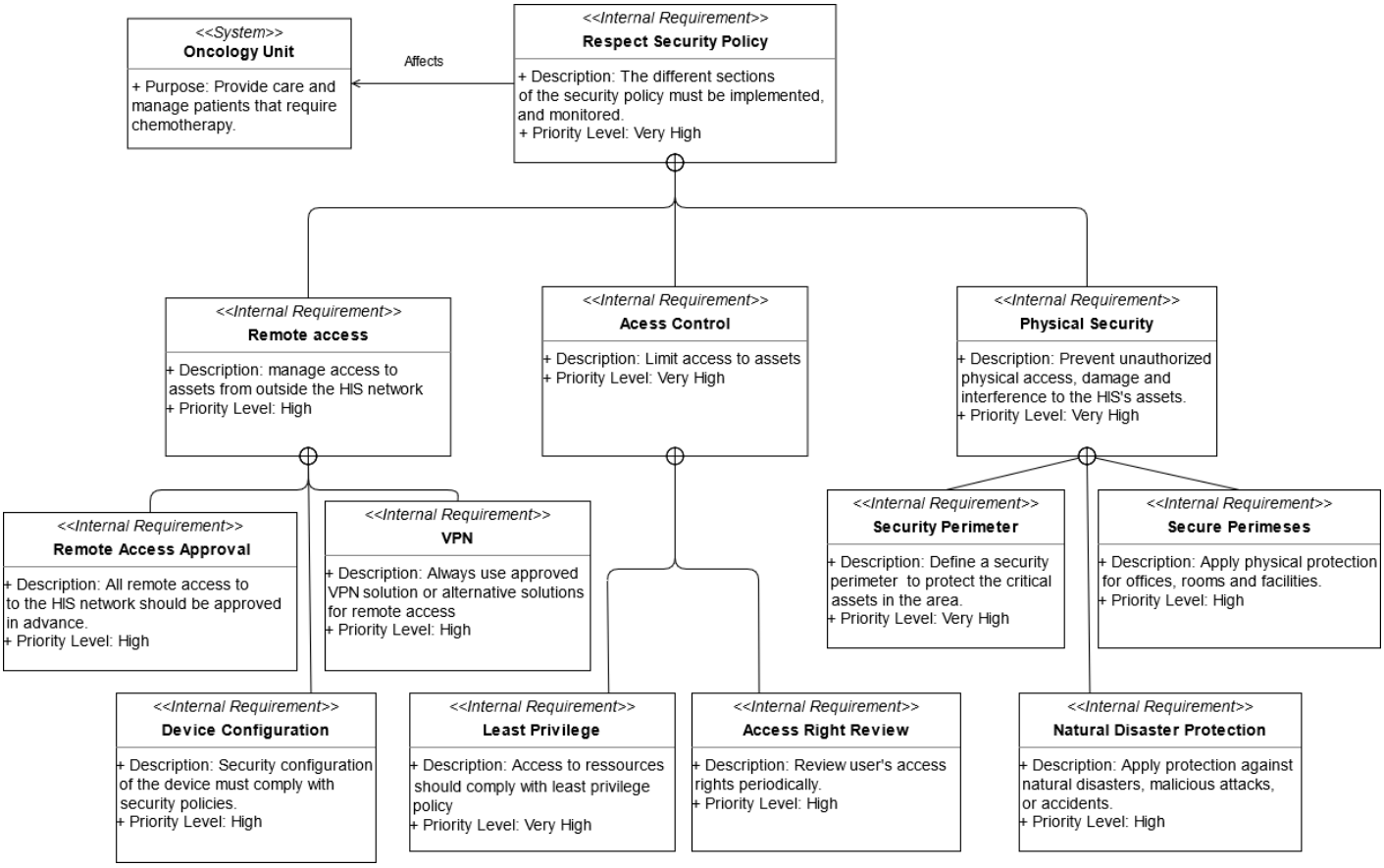


**Fig 5: Hospital Internal security requirement diagram**

insuring the proper realization of the business processes. This equates to the protection of the assets that support process realization and the information they require. The security needs are related to the confidentiality, the integrity and the availability of all assets involved (CIA). Lastly, the HIS high-level security objectives incorporated in the policy stem predominantly from the standard and legislation and reiterate their requirements.

<u>Define security related requirements:</u> After studying the security needs and goals for our case study, we needed to define the security requirements that define the protection to be implemented (Base Practice 10.06). Thus, we translated the objectives and needs of all the previously studied sources to create security requirement diagrams below. The SysML syntax allows the decomposition of requirements until we reach a granularity fine enough to allocate a security control to each security requirement. We translated the high level security goals depicted in the security policy into internal requirements. We also separated standard requirements, depicted as domain requirements, from legal requirements. Lastly, we referred to customer needs as contractual requirements since they are usually contractually binding and can be limited in time depending on the contract. The first diagram (Fig. 5) models some of the requirements that reflect the high level goals of the HIS. Since the policy also defines priority levels for each goal, need or requirement, we added this property to every security requirement. Moreover, the diagram also shows which assets or systems are affected by the security requirements. We implemented this change since, in the SysML specification, requirements affect the entire system whereas that is not the case in security. The diagram of contractual requirement shows this nuance where the requirements for intelligent electronic devices (IED) only affects Hardware such as the servers.

The next diagram regroups some of the requirements that the hospital enforces upon third party equipment providers. Thus, these requirements can be found in the contracts that bind both parties.

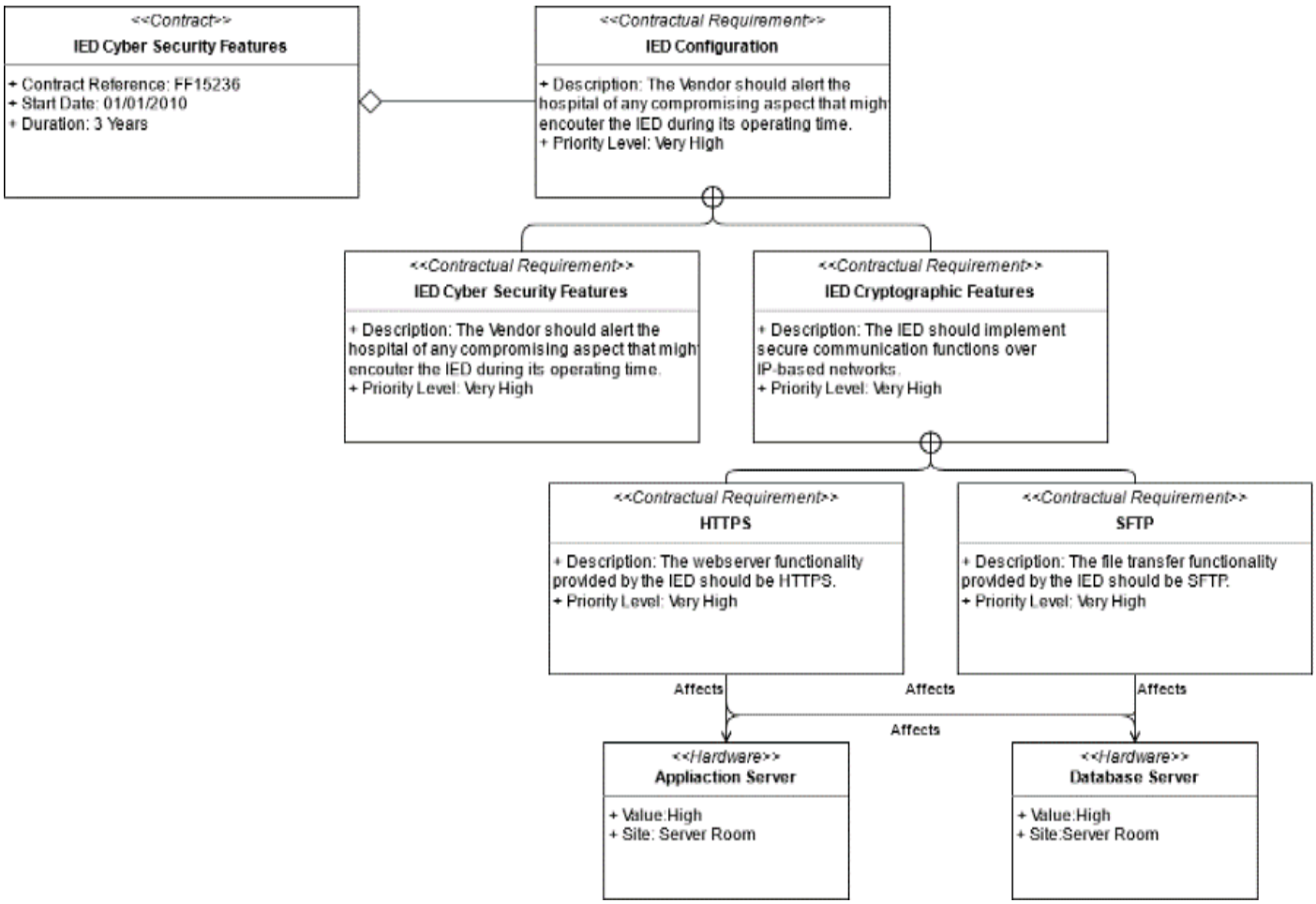


**Fig 6: Hospital contractual security requirements for equipment supplier**

The following diagram (Fig. 7) models the different sections of the ISO 27001 standard. Each section can further be decomposed to reach a leaf security requirement that the HIS can satisfy with security controls. The last diagram showcases the legal requirements mandated by the law 09-08. The model element legal text allows us to refer to the original source document for the legal requirements.

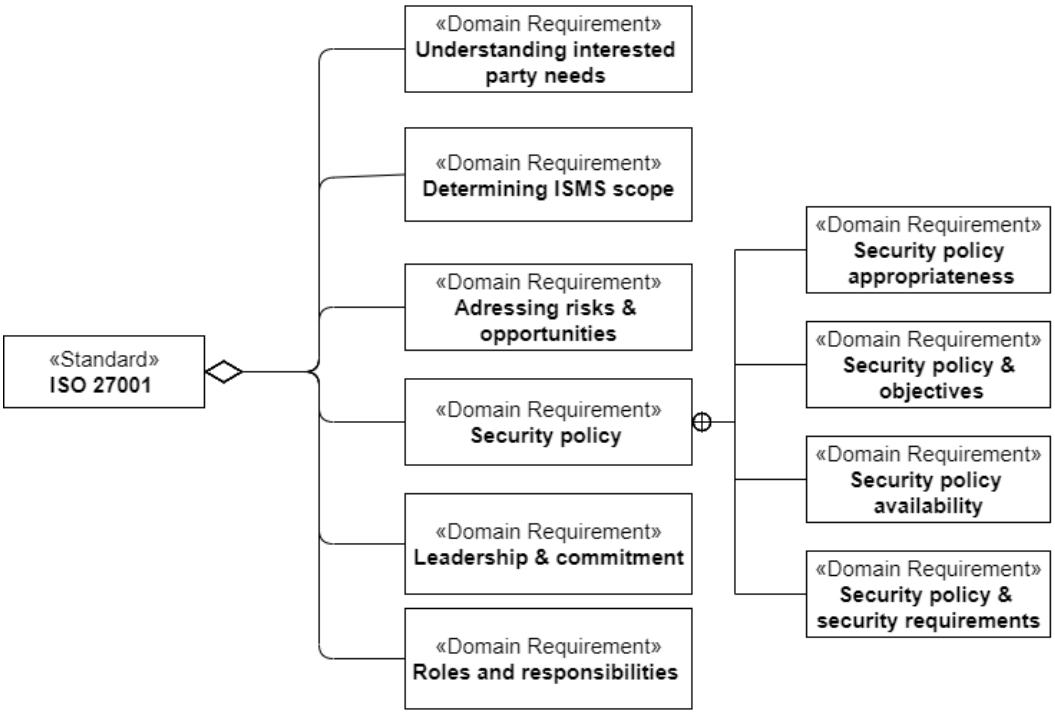


**Fig 7: ISO 27001 Domain security requirements**

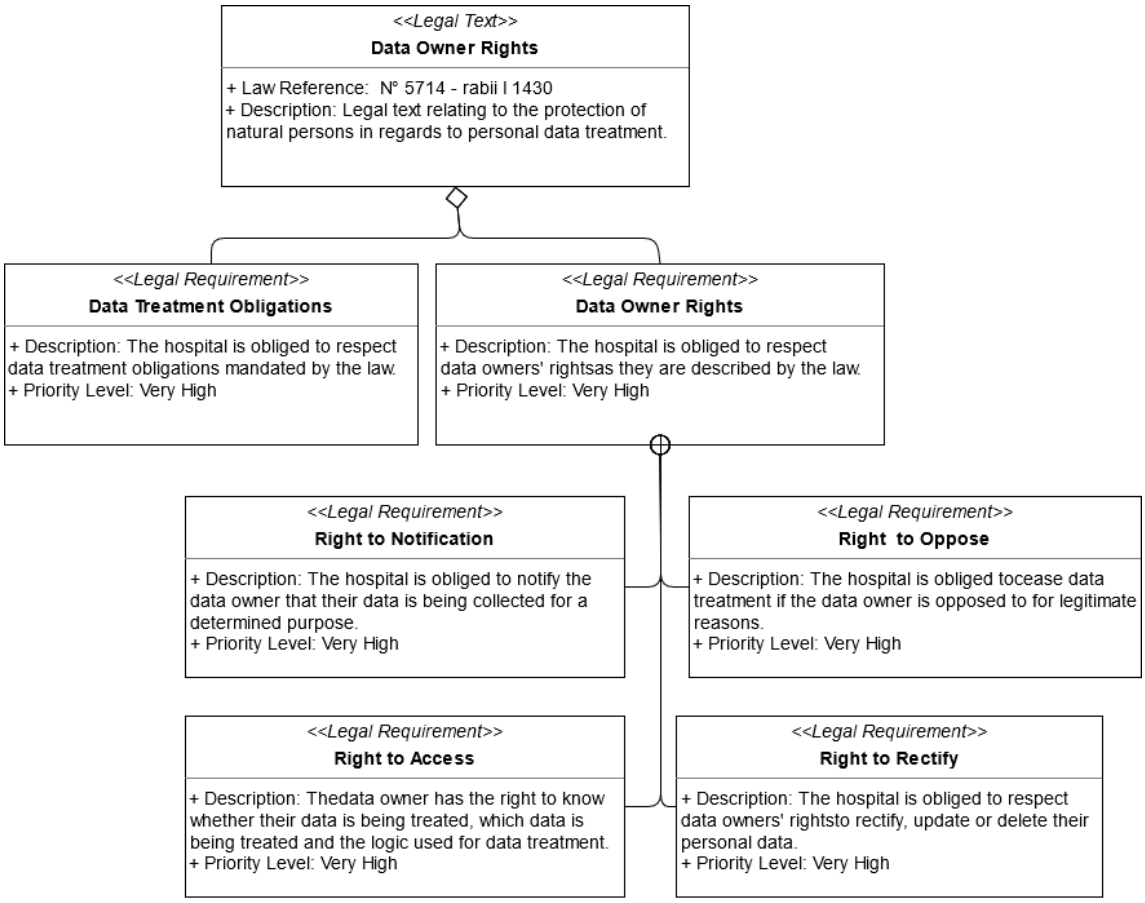


**Fig 8: Legal security requirement diagram**

## Risk Analysis

The first process areas, PA 01 through PA 05, deal with the risk assessment aspect of security. Each of these process areas, even if separate, they are interdependent for the overall risk analysis.

### Assess Vulnerability

We will begin with Process Area 05 that deals with asset vulnerability assessment. It is important to analyze vulnerabilities independently from any threats or attacks since they depend only on the asset itself. Their exploitation by threat agents is something we will assess later through Process Area 04. The standard defines five Base Practices for defining vulnerability analysis methods (BP 05.01), identifying vulnerabilities (BP 05.02), characterizing them (BP 05.03), synthesizing them (BP 05.04) then monitoring them (BP 05.05). In terms of vulnerability assessment, we have access to qualitative and quantitative methods. Qualitative methods include studying attack methodology, philosophy, plans, procedures and scenarios. These methods are used to identify new vulnerabilities that might be exploited later. Quantitative methods are penetration testing based approaches. These methods are best suited to test for known threats that are included in the tests. This analysis should be done on each asset and throughout the system's life cycle. However, these remain choices for the organizations to implement and are not represented by model elements in AtlaSec's risk analysis dimension. However, risk analysis methods can be modeled as security processes. The resulting list of vulnerabilities from analysis is what we propose to model. Thus, we propose the model element "vulnerability" that will be supplemented with vulnerability characteristics and assessments progressively. The vulnerabilities, modeled below, in our case study come from penetration testing, supplemented by the use of tools and available information from CERTs. The most important vulnerability characteristic is its ease of exploitation. The HIS has defined a five-level scale to represent vulnerability levels to make them comparable. This is also practical since the vulnerability levels are an input for risk level measurement. This does not prevent us from adding vulnerability specific characteristics as properties like recommendations. Through vulnerability assessment, we added also added vulnerability descriptions since the results of vulnerability analysis should also be documented. Adding recommendation for each vulnerability is a choice we find interesting, as it can be useful for security control choices. However, some vulnerabilities are the result of existing vulnerabilities. This is what the standard addresses in Base Practice 04. In fact, it is important to aggregate vulnerabilities to avoid overloading risk analysis. In the model, the vulnerability "Wireless communication interception" only exists because of vulnerability "Configuration deficiencies", as highlighted by the composition association. Thus, only the source vulnerability should be treated. Lastly, in terms of vulnerability monitoring, it is a process implemented by the organization that can be modeled as a process rather than an element linked to the vulnerability itself. However, we added temporal information (last measured date,

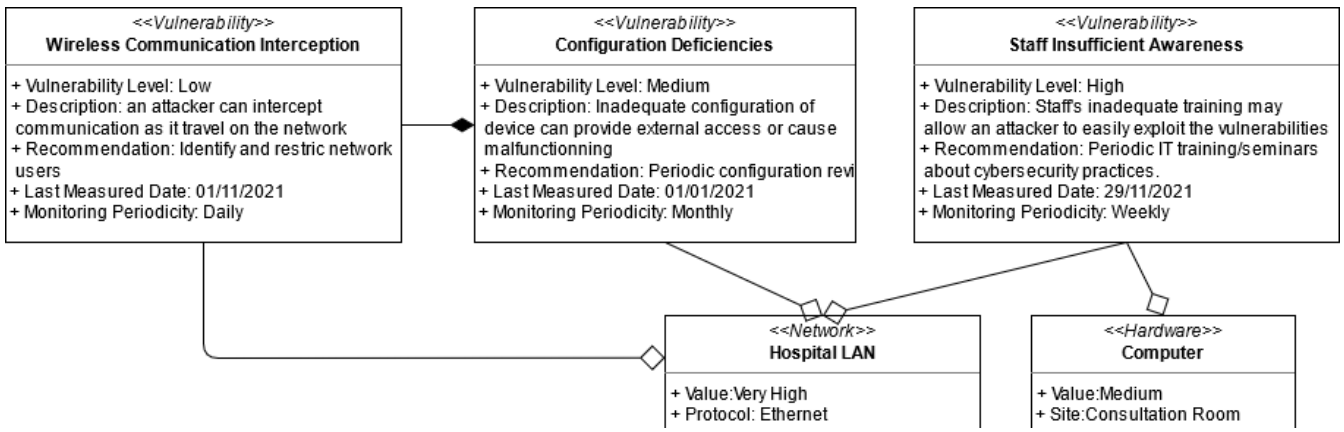


**Fig 9: Security vulnerability diagram**

monitoring periodicity) to vulnerabilities to support monitoring. These properties allow us to run tests with OCL queries to see if vulnerability information needs to be updated. Different verifications can be done at this level, either verifying if there are assets without vulnerabilities or whether some of the vulnerabilities need inspection.

## Assess Threats

Next is Process Area 04 for assessing threats, their properties and characteristics. The standard defines six Base Practices for identifying threats from different sources (BP 01 & 02), a threat measurement scale (BP 03), threat agent capabilities (BP 04), threat likelihood (BP 05) and lastly a threat monitoring process (BP 06). From the study of the base practices, it was evident that we require a model element specifically for threat agents (Base Practice 04). This firstly allows us to distinguish between man-made threats (accidental or deliberate) and natural threats (Script kiddies and rain). Secondly, it allows us to attribute a capability level to each threat agent. This capability is also a scale defined by the HIS similar to the Richter scale for earthquakes or a capability scale reflecting the knowledge of the threat agent. As shown in the diagram, two different threat agents with different skillsets and motives yield threats at different levels. Lastly, this allows for the monitoring of special threat agents. Evidently, we created the model element "Threat" for the identified threats (Base Practice 01 & 02) that will be supplemented progressively with the required characteristics. For natural threats, the hospital was built after having studied natural phenomena occurrences in the area. For example, hospitals in Rabat are built in a safeguarded area in the heart of the city. However, flooding threats, earthquakes and power outages are still realistic threats. On the other hand, man-made threats are more common. Statistically speaking, the number of attacks on critical infrastructure is on the rise from both expert hackers, saboteurs and script-kiddies. Moreover, staff misuse is also a very common threat to consider. Similarly to threat agent capability, threats possess the property "threat level" that reflects the threat unit of measure defined by the organization (Base Practice 03). Again, the HIS uses a five-level scale for calculability. Risk managers make the decision for threat level assessment, as it requires multiple considerations (Base Practice 05). Thus, the modeled threat levels are based on their

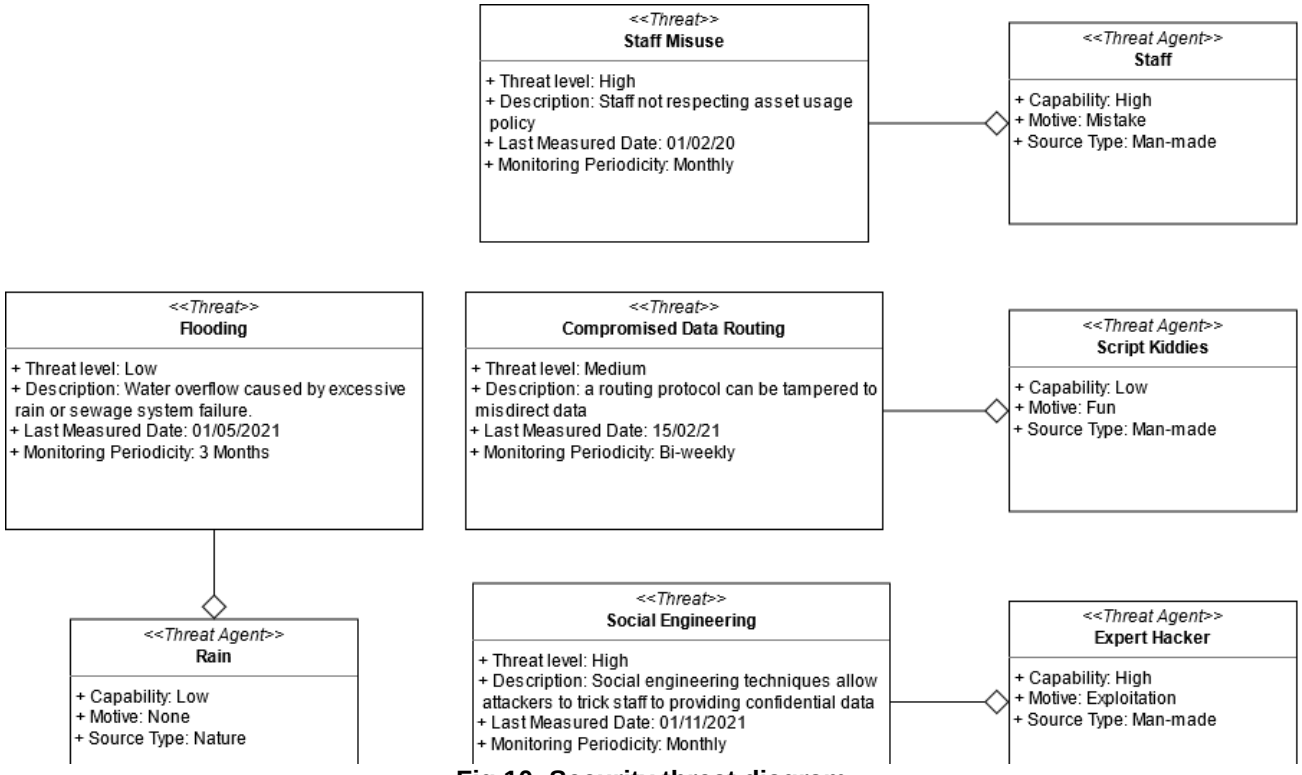


**Fig 10: Security threat diagram**

estimation of the impact the realization of each threat would have on the radiotherapy and pharmacy units. Lastly, to monitor changes in threats and their characteristics, the HIS develops monitoring processes for each set of threats. These processes can be modeled using the "Process" model element but are not directly modeled with the threat. However, we added temporal information (last measured date, monitoring periodicity) to threats to support monitoring. These properties allow testing using OCL (periodicity constraints). Additional verifications include identifying most dangerous threat agents or threat agents that are at the source of many threats.

## Assess Impact

Before addressing security risks, we must assess the impact that any exploitation of vulnerability might have on the system. This is the purpose of Process Area 02 Assess Impact. ISO 21827 defines impact as the consequence of an unwanted incident that affects the system assets. Thus, we must understand what the capabilities (Base Practice 01) and components of the system (Base Practice 02) are to understand how the threats can affect them. However, we have already established in Process Area 10 the processes of our case units and their composition. Thus, we study the impact of incidents on the assets (primordial and support assets) of our case units. Before measuring the impact, we must define the concept of probable incident before assessing its impact. With the model element "Incident scenario", we describe the theoretical exploitation of a vulnerability by a threat. Therefore, it is an association between both model elements. Incident scenario has a calculable incident likelihood that depends on the threat level and the vulnerability level. Then we assess the impact of each incident scenario on each asset. In the example, multiple types of information can be disclosed if communication were to be intercepted. However, patient medical data disclosure is less impactful than public data being disclosed. Thus, impact is also an associative design element between assets and incident scenarios. Using the value of the impacted asset and the likelihood of the incident, we can calculate the impact level. This aligns with the requirements of both Base Practice 03 and 04 since we need to define the operation that calculates the incident likelihood and impact level. Throughout the valuation of each design element, we used five level scales in order to define a matrix to calculate the compound properties. This matrix is presented in Table 1. For example (Fig. 11), the low-level vulnerability wireless communication interception and the high-level threat Compromised data routing yield the highly likely incident scenario data disclosure.

| | **Very Low** | **Low** | **Medium** | **High** | **Very High** |
|---|---|---|---|---|---|
| **Very Low** | Very Low | Low | Low | Medium | Medium |
| **Low** | Low | Low | Medium | Medium | High |
| **Medium** | Low | Medium | Medium | High | High |
| **High** | Medium | Medium | High | High | Very High |
| **Very High** | Medium | High | High | Very High | Very High |

**Table 2: Incident likelihood and impact level calculation matrix**

Similarly, this incident scenario's impact on the very high value asset makes the impact be very high. Moreover, we added to impacts properties suggested by the standard such as type, description, and cost (Bp 05). Lastly, to monitor changes in incident scenarios and impacts, the HIS implements monitoring processes for each design element. These processes can be modeled using the "Process" model element but are not directly modeled with the impact. Since the valuations for impacts and incident scenarios are calculated properties, they will automatically be updated in the model. This removes the possibility of undermining or neglecting

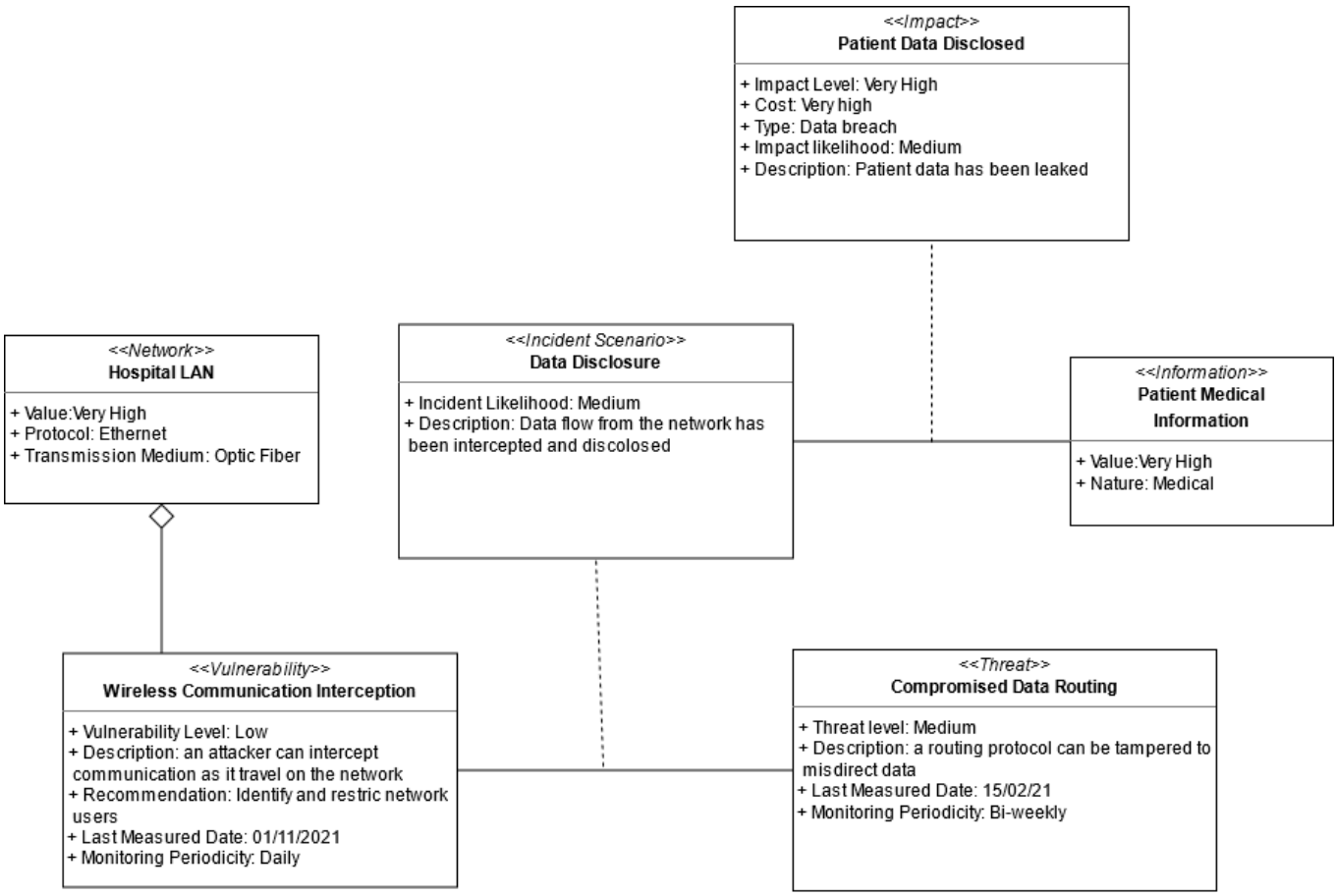


**Fig 11: Security incident impact diagram**

them. Further verifications can be done on the resulting risks directly.

## Assess Security Risks

All these modeled concepts and calculations lead us to the risk assessment in Process Area 03. The security risks are the likelihood that the impact of an unwanted incident scenario will be realized. Security risks are specifically related to the previously modeled impacts for each primordial and support asset. The standard defines six Base Practices that encompass risk-measuring methods (Base Practice 03.01), identifying exposures (Base Practice 03.02), assessing uncertainty (Base Practice 03.03), prioritization (Base Practice 03.05) and risk monitoring. Firstly, the risk evaluation methods are put in place by the organization (BP 03.01). The results of these methods should also allow comparison and prioritization. For the HIS in our case study this method depends on the impact level previously calculated and the input of risk managers. The risk managers can classify risks at a higher level than the calculated estimate. This risk assessment is what we seek to comply with Base Practice 03.03. Thus, the risk level is calculated automatically according to the impact level. Moreover, we added properties such as risk taxonomy (financial, operational, strategic, business, reputation ...) and acceptance level. In the example provided below, we want the risk "Patient Information Disclosed" to be reduced to the level "very low" at least. Furthermore, the risk assessment yields another organized five level scale. As shown in the risk diagram, the priority is given by the risk level itself. This prioritization satisfies the requirement of Base Practice 03.05 since it takes into consideration vulnerability, threat and asset valuations. Moreover, the advantage of modeling all the aspects of Process Areas 05, 04 and 02 is that we trace back the exposure at the source of the risk i.e. the triplet {threat, vulnerability, impact} (BP 03.02). Therefore, identifying an adequate solution adapted to the exposure is further facilitated. Thus, the risk diagram presented below is an extension of the

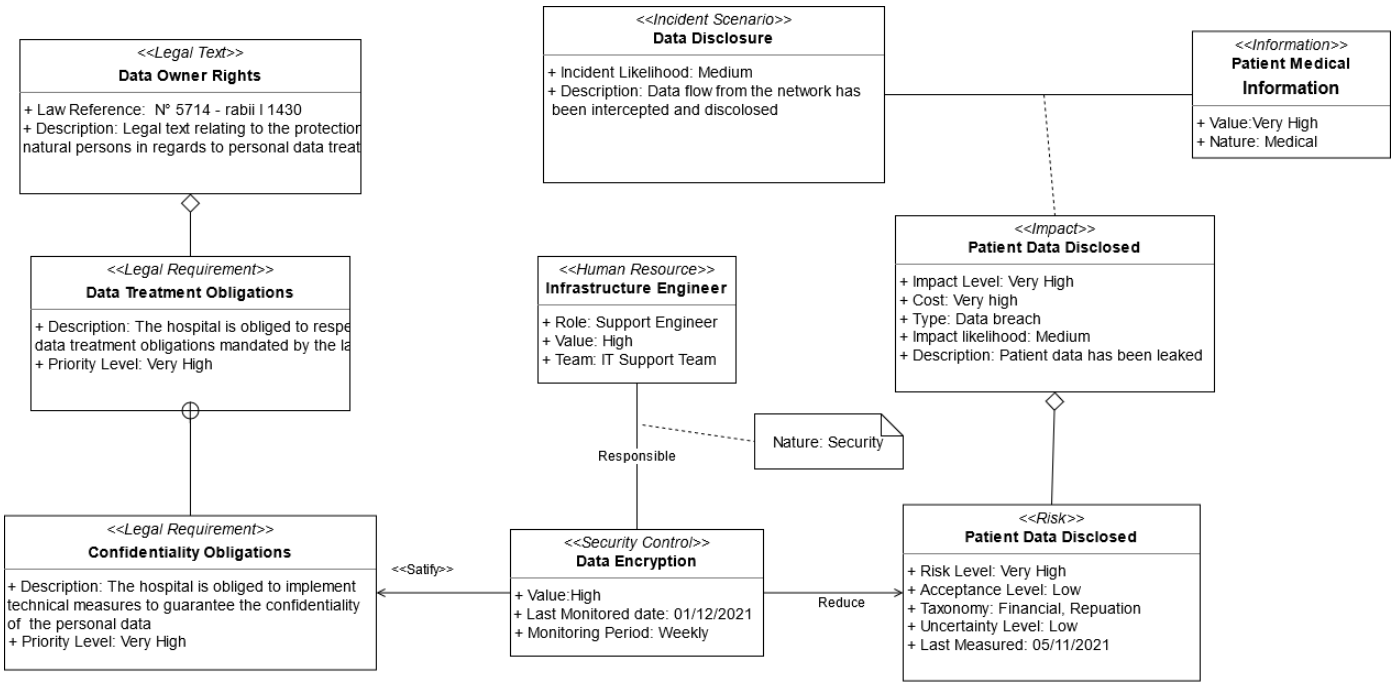


**Fig 12: Implemented security control diagram**

previous diagram in Fig 12. Evidently; each risk will have uncertainty associated to it (BP 03.04). It represents the aggregation of all the uncertainties in the assessments that led up to it. It is important for assurance to take uncertainties into consideration since no assessment is immaculate. Thus, we added the property "uncertainty level" to each risk. Lastly, to monitor risk changes, the HIS implements monitoring processes for each risk such as monitoring network traffic. These processes can be modeled using the "Process" model element but are not directly modeled with the risk. It is still necessary to verify the state of the risk through analyzing its sources. We have added temporal properties to the design element "risk" in order to support the monitoring process used.

## Administer Security Controls

To conclude risk analysis, Process Area 01 handles the administration of security controls for risk reduction. The standard defines base practices to establish responsibilities for controls (BP 01.01), manage their configuration (BP 01.02), manage awareness and training (BP 01.0.3) and manage maintenance (BP 01.04). By design, we defined security controls as assets that have the function of reducing risks or satisfying requirements. As a specialization of assets, all security controls can be assigned one or multiple responsibilities. However, there is a condition in terms of skill; the skill level of the human resource should match that of the asset. This allows us to maintain accountability for the proper functioning and configuration for all security controls. Additionally, we added OCL constraint specifying that all security controls must at least have one responsible (Base Practice 01.01). The remaining Base practices of this Process Area require the implementation of processes for configuration, training and monitoring. These processes can be modeled using process diagrams or activity diagrams. To this end, we have implemented temporal properties for the security controls to support monitoring. The risk diagram below groups the model elements for both risk assessment and administering security controls. Since all design elements have a monitoring periodicity, exceeding this deadline will flag the design element thus launching a chain of events leading up to the risk level not being at the desired state and requiring intervention. This interconnection between all these model elements is what guarantees the production of insurance at the level of the risk analysis dimension. Any alteration such as adding a new asset, removing a security control or even a human resource will create a gap leading to a gap

(an asset without a responsible, an unprotected asset or tasks that should be reassigned) necessitating intervention.

## Verify and Validate Security

Process Area 11 addresses the satisfaction and verification of the defined security requirements. The objective of this process area is to ensure that the solutions implemented are verified and validated. Thus, the process area handles identifying security solutions (Base Practice 11.01), defining verification and validation approaches (Base Practice 11.02), performing verifications (Base Practice 11.03), performing validations (Base Practice 11.04) and providing their results (Base Practice 11.05). In terms of identifying the security solutions (BP 11.01), this is provided through distinguishing security controls from regular assets. By definition, security controls are the design elements created to satisfy security requirements and reduce security risks. Thus, they will be the target of verification and validation. Next, we need to identify the test procedures for each security control's verification and validation (BP 11.02). These are determined by the IT support team at the hospital. They range from test procedures to re-evaluating previous penetration tests post security control implementation. As a matter of design, they are model as "Security Evaluation Mechanisms". This model element is an extension of the SysML model element "test case" that serves to "verify" the satisfaction of a given security requirement. In the previously modeled diagram, we modeled the legal confidentiality obligations requirement and the security control that satisfies it. In this case, the security evaluation mechanism is a means to verify that the data encryption implemented serves its purpose. This is done according to the Cryptographic Algorithm Validation Program (CAVP) where NIST provides a list of certified implementation solution. As a result, upon performing the required verification and validation (BP 11.03 & 11.04), the security control is either kept in use or changed. Thus, the results of the verification and the validation of the security requirement's satisfaction are updated using the properties of the verify association (BP 11.05). Lastly, SysML-based models are modular and re-purposable since adjustments can be made to the meta-model to adapt to the specific context. This modularity allows for greater flexibility and customization in the security evaluation process, ensuring that the models can be tailored to the requirements and processes of different environments.

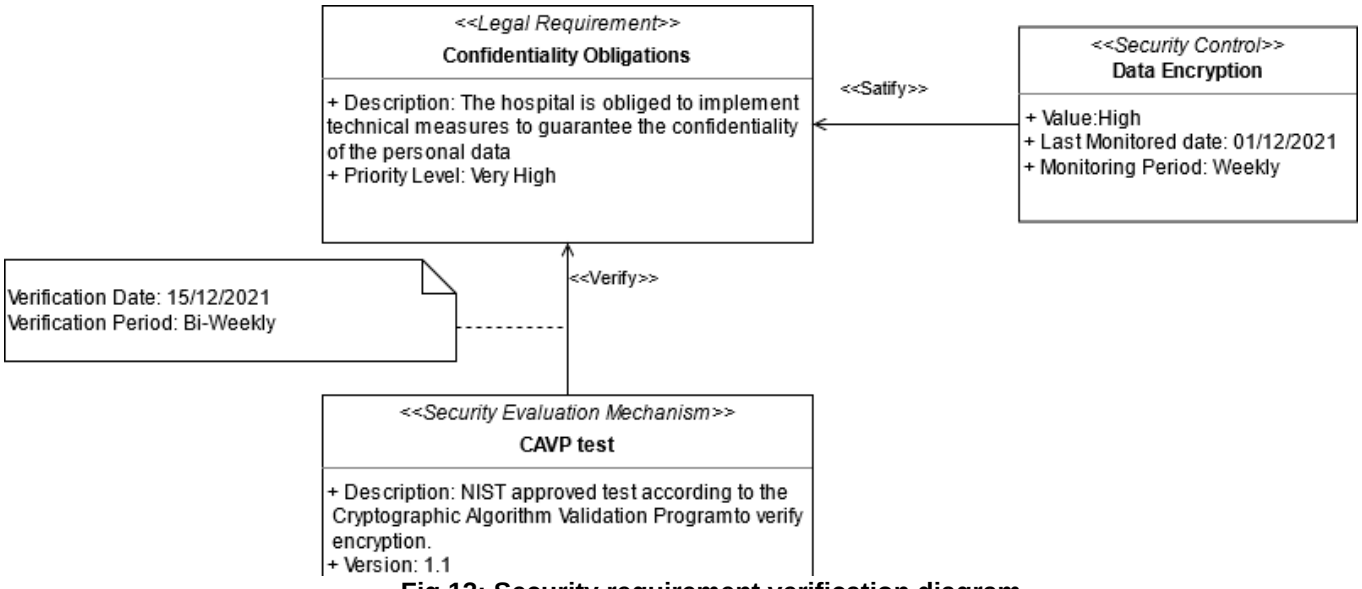


**Fig 13: Security requirement verification diagram**

## Monitor Security Posture

Process Area 08 addresses the monitoring effort of the entire security posture. The purpose is to ensure that gaps, mistakes, breaches and attempted breaches are identified and dealt with. This translates into monitoring all the aspects discussed in earlier process areas. In fact, the base practices of this process area handle event analysis (BP 08.01), change monitoring (BP 08.02), incident identification (BP 08.03), security control monitoring (BP 08.04), security posture review (BP 08.05), incident response (BP 08.06), and monitoring asset protection (BP 08.07). Most of these practices have been addressed individually throughout the previous process areas. In fact, while analyzing event records to extract exposures is a process to model independently (BP 08.01), the model elements presented in the risk analysis diagrams support this base practice. The results of this analysis are the inputs to the aforementioned qualitative methods for vulnerability or threat identification. Similarly, the base practice 08.03 is also encompassed by the design element "Incident Scenario". As for monitoring in base practice 08.02 and 08.04, we have added temporal properties to all design elements from system composition to risk analysis including security controls. However, it is the duty of the organization to implement monitoring processes and update the modeled information. Once the deadlines are exceeded, it leads to a snowball effect of required re-evaluations in order to determine whether these assessments are still valid. This leads to the requirement of the next base practice which is reviewing the security posture. This review translates to the verification that all the modeled security requirements all the security risks are complete and unchanged. This is one of the strong points of the having modeled these security concepts. The security diagrams are a concise and organized platform to append these changes and witness the effect of these changes ripple through the diagrams identifying future tasks needed. For example, increasing the acceptance level of a security risk should put into question the effectiveness of the implemented security control. In the case of incident response for BP 08.06, the security diagrams provide the proper input to create continuity and recovery plans. In fact, the diagrams identify the critical business processes, assets and security controls. Lastly, monitoring assets and artefacts (BP 08.07) are still considered assets of the system and thus they will be protected according to their criticality level. They will be subjected to the same treatment as any other asset as seen in Process Areas 01 through 05.

## Build Assurance Argument

Process Area 06 addresses the assurance argument that conveys to the client that their needs have been met. It consists of a set of evidence that supports the stated assurance objectives laid out by the customer. These are the same security needs we have extracted and modeled in Process Area 10. Process Area 06 seeks to identify the security assurance objectives (Base Practice 06.01), define a strategy to address them (Base Practice 06.02), monitor them (Base Practice 06.03), identify assurance evidence (Base Practice 06.04), analyze the evidence (Base Practice 06.05) and provide assurance argument (Base Practice 06.06). In terms of modeling, the assurance objectives are the previously modeled security requirements. In defining the security assurance objectives, the customer must specify the level of confidence required in the security policy implemented. Thus, this translates as a need to have the client approve the modeled security requirements. Next, the strategy defined by the organization is a plan that encompasses the plethora of choices it will implement to secure its system. Thus, the assurance strategy must take into consideration all the modeled security requirements and the security risks. As a result, our diagrams provide a comprehensive platform to elaborate this strategy without leaving out any requirements. Then, the realization of the assurance strategy are the modeled security controls implemented to satisfy each requirement. Thus, the evidence is proof that the security controls are properly functioning. This relates to monitoring through security evaluation mechanisms for each requirement. The result of these evaluation mechanisms constitutes the basis of the assurance argument. Since each evaluation mechanism is monitored for changes and periodically reassessed,

this guarantees a timely assurance argument for the customer.

## Coordinate Security & Provide Security Input

The last two Process Areas 09 and 07 include aspects that cannot be modeled yet can be supported by the modeled elements. Firstly, the goal of Process Area 09, Provide Input, is to provide the necessary information about the system, its components, security requirements, and security state to its different actors. The entirety of the modeled concepts provide engineers, designers and decision makers with the necessary information and the scalable view of the system. Similarly, Process Area 07 emphasizes on the coordination between different actors to resolve conflicts and make decisions as a unit. This is where our solution falters: where these cannot be modeled or assessed at this scope since they are at the implementation level. However, the models provide a map that serves as a means of communication and an instigator of discussion.

The table below (Table 3) summarizes the base practices covered in each process area specifying whether their requirements are implemented as model elements, covered by the diagrams or not implemented.

**Table 3: Coverage of base practices by the AtlaSec method**

| Process Area | Base Practice | implemented through a design element | Covered by the diagrams | Not Implemented |
|---|---|---|---|---|
| Process Area 01 Administer Security Controls | Establish security responsibilities | X | | |
| | Manage security configuration | | | X |
| | Manage security awareness, training, and education programs | | X | |
| | Manage security services and control mechanisms | | X | |
| Process Area 02 Assess Impact | Prioritize capabilities | X | | |
| | Identify system assets | X | | |
| | Select Impact metrics | | X | |
| | Identify metric relationship | X | | |
| | Identify and characterize impacts | X | | |
| | Monitor Impacts | | X | |
| Process Area 03 Assess security risk | Select risk analysis method | | X | |
| | Exposure identification | X | | |
| | Assess exposure risk | X | | |
| | Assess total uncertainty | X | | |
| | Prioritize risks | X | | |
| | Monitor risks and their characteristics | | X | |
| Process Area 04 Assess threat | Identify natural threats | X | | |
| | Identify man-made threats | X | | |
| | Identify threat units of measure | X | | |
| | Assess threat agent capability | X | | |
| | Assess threat likelihood | X | | |

| | | | | |
|---|---|---|---|---|
| | Monitor threats and their characteristics | | X | |
| Process Area 05 Assess vulnerability | Select vulnerability analysis method | | X | |
| | Identify vulnerabilities | X | | |
| | Gather vulnerability data | X | | |
| | Synthesize vulnerabilities | X | | |
| | Monitor vulnerabilities and their characteristics | | X | |
| Process Area 06 Build assurance argument | Identify assurance objectives | X | | |
| | Define assurance strategy | | X | |
| | Define security measures | X | | |
| | Control assurance evidence | X | | |
| | Analyze evidence | | | X |
| | Provide Assurance argument | | X | |
| Process Area 07 Coordinate security | Define coordination objectives | | | X |
| | Identify coordination mechanisms | | | X |
| | Facilitate coordination | | X | |
| | Coordinate security decisions and recommendations | | | X |
| Process Area 08 Monitor security posture | Analyze event records | | X | |
| | Monitor changes | | X | |
| | Identify security incidents | X | | |
| | Monitor security safeguards | | X | |
| | Review security posture | | X | |
| | Manage security incident response | | | X |
| | Protect security monitoring artifacts | | X | |

| | | | | |
|---|---|---|---|---|
| Process Area 09<br>Provide security input | Understand security input needs | X | | |
| | Determine security constraints and considerations | X | | |
| | Identify security alternatives | | | X |
| | Analyze security of engineering alternatives | | | X |
| | Provide security engineering guidance | | | X |
| | Provide operational security guidance | | | X |
| Process area 10<br>Specify security needs | Gain understanding of customer security needs | X | | |
| | Identify applicable laws, policies and constrains | X | | |
| | Identify security context | X | | |
| | Capture security view of system operation | X | | |
| | Capture high level security goals | X | | |
| | Define security related requirements | X | | |
| | Obtain agreement on security | | X | |
| Process Area 11<br>Verify and validate security | Identify verification and validation targets | X | | |
| | Define verification and validation approach | X | | |
| | Perform verification | | X | |
| | Perform validation | | X | |
| | Provide verification and validation results | X | | |

# Conclusion & Lessons Learned

This study focused on evaluating the applicability of the AtlaSec methodology in the context of the audited HIS. The attained results show substantial improvement of the apprehension of security in such a complex context. The basis of the methodology itself improved during the different implementation iterations to finally reach a version that supports most of the essential practices for all process areas. However, the impact of the support provided is not evenly distributed along all process areas. For process areas 01 to 05, the application of models to represent security risk analysis helped better understand the nature of threats as well the definition of strategies depending on what the sources were: some risks are better dealt with through their perpetrators i.e. threat agents. In addition, the models highlight the chain of consequences of some events within the system such as a deficient asset or a new incident. Similarly, modeling system composition as a map of interacting assets helps understand the consequences of composition complexity: the surrounding assets can also be seen as points of entry regardless of the security invested in the main asset. The methodology also helps optimize the choices of security controls for both risk reduction and security requirement satisfaction. Thus, the objectives for process areas 06, 10 and 11 are reached, allowing a formal provision of insurance for the organization and its clients. On the other hand, the support for process areas 07 and 09 is less instrumental since they both rely heavily on processes defined during implementation. Yet, AtlaSec still provides a platform that consolidates all the information required for inputs and collaboration.

The choice of method is well suited for this study – as opposed to experiments, surveys, or action research – since the lines between security, complexity and the context of the study are blurred. In addition, it provides necessary flexibility due to the nature of the subject and the data being of qualitative nature. Informality was inevitable especially to allow for improvement iterations. We learned to balance between this informality for qualitative analysis and following the research methodology and audit processes. Moreover, the same study can be performed from multiple point of view either to dive deeper into the exploration of the intervention at the HIS itself or repeat the same study in a different context to support generalization. With different objectives, we can define different research questions and reorient the study depending on findings or the context. However, the support of ITRoad was crucial to the success of the study. Their involvement provided a contact with different actors in the HIS with the support of its top management. Their expertise provides the necessary expertise to carry out the missions and to confirm results. It is highly beneficial to the improvement of the solution to use the case as a basis when seeking an agreement or gap identification. It creates a concrete starting point for discussions rather than abstract argumentation. Furthermore, cause-effect analyses are difficult to ascertain with the use of a supporting tool since its effect is amalgamated with factors such as understanding of the solution and its integration with the existing solutions. However, according to Kitchenham (Kitchenham, Dyba, & Jorgensen, n.d.), these are problems that affect all case studies and are accepted in this context.

For future studies, we intend to increase the number of case units. This allows for a more diverse verification of the applicability of the AtlaSec methodology. We also plan to upgrade from a prototype of a modeling tool to a dedicated modeling platform. This would improve user experience and facilitate adding new features such as data based reports or machine learning based gap analysis.

# Acknowledgements

The authors gratefully acknowledge **IT Road** for their active involvement in the audit process and for the provision of the data necessary for this research. Particular thanks are extended to **R. Ressani** for his cooperation, availability, and valuable contributions, which materially supported the rigor and completion of this study.

# References


Anass, R., Saliha, A., Khadija, O. T., & Ounsa, R. (2019). *A Comparison of American and Moroccan Governmental Security Approaches*. https://doi.org/10.1007/978-3-030-03577-8_39

Anass, R., Saliha, A., & Ounsa, R. (2020). A Concept & Compliance Study of Security Maturity Models with ISO 21827. *Proceedings of the 22nd International Conference on Enterprise Information Systems*, 385–392. SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0009569703850392

Assoul, S., Rabii, A., & Roudiès, O. (2021). An Operational Responsibility and Task Monitoring Method: A Data Breach Case Study. *Advances in Science, Technology and Engineering Systems Journal*, *6*(1), 1157–1163. https://doi.org/10.25046/aj0601130

Bertin, J. (1987). Semiology of graphics: diagrams, networks, maps. In *he University of Wisconsin Press*. Madison.

DGSSI. (2013). Directive Nationale de la Sécurité des Systèmes d'Information,. Retrieved from https://www.dgssi.gov.ma/sites/default/files/attached_files/directive_nationale_de_la_securite_des_systemes_d_information.pdf

Fuller, R. B. (1957). *A comprehensive anticipatory design science*. *34*, 357–361.

Harel, D., & Rumpe, B. (2004). Meaningful modeling: what's the semantics of "semantics"? *Computer*, *37*(10), 64–72. https://doi.org/10.1109/MC.2004.172

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and F. S. (2015). *Cyber Readiness Index 2.0*. Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-index-2.0-web-2016.pdf

ISO/IEC. (2013). ISO 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Retrieved from https://www.iso.org/standard/54534.html

ISO/IEC. (2018). ISO 27005:2018 Information technology — Security techniques — Information security risk management. Retrieved from https://www.iso.org/standard/75281.html

ISO. (2008). *ISO/IEC 21827:2008(en) Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)* (p. 144). p. 144. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:21827:ed-2:v1:en

ISO. (2013). *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*. Retrieved from https://www.iso.org/standard/54533.html

Jabbar, S., Lahboube, F., Souissi, N., & Roudies, O. (2017). Optimisation de la cartographie des processus du système d'information de l'Hôpital Militaire d'Instruction Mohammed V. *Santé Publique*, *29*(3), 371. https://doi.org/10.3917/spub.173.0371

Javaid, M. I., & Iqbal, M. M. W. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). *2017 International Conference on Communication Technologies (ComTech)*, 78–90. IEEE. https://doi.org/10.1109/COMTECH.2017.8065754

Kitchenham, B. A., Dyba, T., & Jorgensen, M. (n.d.). Evidence-based software engineering. *Proceedings. 26th International Conference on Software Engineering*, 273–281. IEEE Comput. Soc. https://doi.org/10.1109/ICSE.2004.1317449

Luis Enrique Sánchez, Daniel Villafranca, P. M. (2007). MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. *Proceedings of the 5th International Workshop on Security in Information Systems*, 233–244. SciTePress - Science and and Technology Publications. https://doi.org/10.5220/0002430402330244

Moody, D. (2009). The "Physics" of Notations: Toward a Scientific Basis for Constructing Visual Notations in Software Engineering. *IEEE Transactions on Software Engineering*, *35*(6), 756–779. https://doi.org/10.1109/TSE.2009.67

Mubarak, S.; Heyasat, H.; Wibowo, S. (2019). . Information Security Models are a Solution or Puzzle for SMEs? A Systematic Literature Review. *In*

*Proceedings of the Australasian Conference on Information Systems.*, 148–154. Perth, Australia.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.04162018

North American Electric Reliability Corporation. (2015). NERC Critical Infrastructure Protection Standards. Retrieved from https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Novaes Neto, N., Madnick, S. E., Moraes G. de Paula, A., & Malara Borges, N. (2020). A Case Study of the Capital One Data Breach. *SSRN Electronic Journal*, (January), 0–24. https://doi.org/10.2139/ssrn.3542567

Ponsard, C., Massonet, P., Grandclaudon, J., & Point, N. (2020). From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 75–78. IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00019

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Rabii, A., Assoul, S., & Roudies, O. (2020). Security requirements elicitation: A smart health case. *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, 776–781. https://doi.org/10.1109/WorldS450073.2020.9210330

Road, I. (n.d.). IT Road Consulting. Retrieved from http://www.itroad.ma/

Teufel, S., Teufel, B., Aldabbas, M., & Nguyen, M. (2020). *Cyber Security Canvas for SMEs*. https://doi.org/10.1007/978-3-030-66039-0_2

Verizon Business. (2021). *Data Breach Investigations Report (DBIR) 2021*. Retrieved from https://www.verizon.com/business/en-gb/resources/reports/dbir/

White, G. B. (2011). The community cyber security maturity model. *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, 173–178. IEEE. https://doi.org/10.1109/THS.2011.6107866

Yulianto, S., Lim, C., & Soewito, B. (2016). Information security maturity model: A best practice driven approach to PCI DSS compliance. *2016 IEEE Region 10 Symposium (TENSYMP)*, 65–70. IEEE. https://doi.org/10.1109/TENCONSpring.2016.7519379