

Article

Security Requirements Engineering Framework with BPMN 2.0.2 Extension Model for Development of Information Systems

Saima Zareen ^{1,*}, Adeel Akram ¹ and Shoab Ahmad Khan ²

¹ Faculty of Telecom and Information Engineering, University of Engineering and Technology, Taxila 47050, Pakistan; adeel.akram@uettaxila.edu.pk

² Department of Computer and Software Engineering, National University of Sciences and Technology, Islamabad 46000, Pakistan; kshoab@yahoo.com

* Correspondence: saima.zareen@uettaxila.edu.pk

Received: 17 June 2020; Accepted: 15 July 2020; Published: 20 July 2020



Featured Application: This work can be applied with the Requirements Engineering Process to elicit the security requirements for an information system's development.

Abstract: With recent advancements of technologies such as Internet of Things and cloud computing, security of information systems has emerged as a critical issue. This has created a need for elicitation and analysis of the security requirements at an early stage of system development. These requirements should also be expressed using visual notations that can encapsulate the vision of different stakeholders related to security. While business process management notation (version 2.0.2) is a widely used graphical representation for business requirements and makes it easier to define and communicate business processes between different stakeholders of the system. Moreover, extension mechanisms are available to model the specific needs of an organization. Due to its flexible structure for defining new extensions, it can be adapted to model security requirements in the information system (IS). Towards this, we propose a threat profile security framework to define the security requirements of manufacturing systems for businesses, which are at a stage of infancy to adapt or evolve the IS with the changing needs of a business environment. In particular, the framework is modeled by extending Business Process Management Notation and is applied in a manufacturing industry process at the shop floor level. We show through a case study example that the threat goal-based framework is broader and, hence, covers a majority of security concerns of organizations.

Keywords: security requirements; business process management notations (BPMN); manufacturing; security threats; security goals; information systems; enterprise resource planning

1. Introduction

Enterprise Resource Planning Systems (ERPs) is the technology that provides the unified business functions to organizations by integrating their core processes. ERPs have been used in different businesses such as energy sector, manufacturing, Information Technology (IT), education, and banking [1]. For instance, in the manufacturing industry, it is used for forecasting the production rate based on the data from different sources to manage inventory and produce orders for raw materials, develop production schedules, time tables for shifts, and draw financial projections [2]. All these systems rely on data that is stored at different locations. Hence, issues related to data consistency, integrity, and availability arise. Businesses are extending their services by providing mobile applications that are available to users to fulfill their needs and increase business value [3]. There is risk associated with every technology-based solution whether these are used personally in mobile applications or used

by different stakeholders in enterprises systems. With the evolution of technology, ERP is undergoing transformation, such as cloud-based ERPs, Internet of Things (IoTs), and the emerging industry 4.0 revolution. Moreover, business transactions are being converted to bitcoin and e-wallet systems [4]. All these transformations require highly integrated, more intelligent, and more collaborative systems in organizations [5,6], where the role of ERPs is more focused on accuracy, performance, and security rather than just providing information and data services. Provision of the ERP security is more complex due to people who use the ERP system, viruses, network availability, confidentiality, and integrity problems [7]. There are various ERP vendors including Oracle, SAP, Microsoft, and Sage. They are using role-based access control, extended role-based access control, and logging details of users and their activities at the application layer [8,9]. Vulnerabilities like default accounts and passwords, no encryption on sensitive data, and poor password control have been found in existing ERPs such as Oracle e-business suite [10]. Thus, ERP systems are becoming highly vulnerable, where security considerations should be critical [8]. It is important to identify how existing ERPs can address security concerns of manufacturing sector for their manufacturing plants security, robot's protection, sensors protection, and protection of hybrid connected devices. To this end, existing information systems cannot solve security issues when used in smart manufacturing industry [11,12]. In particular, when a small error can result in huge monetary as well as loss of human life, which would significantly damage a company's credibility.

There are several standards developed for ensuring security in information systems (IS) by organizations such as ISO 27001 [13], National Institute of Standards and Technology NIST Special Publication SP800-53 [14], Common Criteria (CC) [15], and Control Objectives for Information Technologies (COBIT) [16]. These standards have defined controls, security policies, conformance, and integration of these procedures with an organization's daily operations. For most cases, a standard recommends other standards for taking a benefit from it completely. It is not possible for an organization to achieve assurance according to all these security standards. These standards have complex procedures and heavy costs. Hence, there is a need for customized standards and procedures to implement a secure ERP system in accordance to a company's needs.

Security requirements include security goals such as confidentiality, availability, integrity, accessibility, and accountability of the system. In most cases, a requirement engineer would consider encryption, authentication, and access control mechanisms as security requirements. These requirements are replaced with architectural or design constraints. It is very common to include security requirements only after the system has been designed. This results in a problem of overfitting security requirements in the existing design that lead to emergence of computer systems with security vulnerabilities. These security problems can only be removed by integrating security with the requirements engineering (RE) process, which requires that the security requirements are gathered using well-defined processes. Such practices would help in the analysis of alternative options to be implemented in the systems. To this end, a security requirement engineering process should consider the security requirement as a functional requirement and include activities to elicit them like functional requirements [17] such as:

- Identify assets, threats, and vulnerabilities,
- Model the possible threats to the system to specify its security features,
- Risk analysis by considering the security assessment method,
- Security requirements specification using specification language or modeling,
- Requirements specification reviews to find security errors.

There are different security requirement engineering processes such as Software Quality Requirements Engineering Process (SQUARE) [18], Security Requirements Engineering Process (SREP) [19], and Secure TROPOS [20,21], which is a tool to model goal-oriented requirements and knowledge acquisition in automated specification (KAOS) [22] including misuse cases [23] and security-based Unified Modeling Language (secUML) [24]. Most of these processes have a similar

set of security requirement engineering activities. These processes can be used to identify security requirements to evaluate them based on priority and cost. The effectiveness of security requirement engineering lies in its usage and popularity, but very few applications of these processes have been found.

Existing security research enforces security requirements at the design, implementation, or maintenance phase. In Reference [25], it was shown that security research emphasized network security (i.e., 43.7%), and very low attention was given to security authentication systems (i.e., 6.8%). Other security research fields are content leakage prevention mechanisms, user terminal security systems, cryptography, intrusion detection, cyber-attack detection, and information system security. However, researchers have found that human interaction with these systems is the real cause of most breaches [26,27]. This human factor is called an agent, which purposely exploits weaknesses of the system or unintentionally uncovers vulnerabilities either by using the system, or by using mobile devices that can leak and exploit sensitive information to other people [27].

Various techniques and frameworks have been proposed to assess the risk caused by threats to critical assets and to define their countermeasures [19]. These efforts do not end in defining security requirements and designing systems accordingly. It is required that the security of the system should be assessed according to the new threats introduced in the recurring system [28]. There is also the need to perform risk analysis to evaluate the security state of a system in an event of a change. Provision of security in IS requires a full process, where it requires us to identify threats continuously. Threats are known to be dynamic and a similar threat can be applied at different layers of an IS for different purposes [29–31]. Most studies [32–36] have shown that security threats are the main part of every security framework and security standard.

The security requirement engineering process requires models to present threats for analysis. For this purpose, we have two standard Business Process Management Notation 2.0.2 (BPMN) and Unified Modeling Language UML defined by the Object Management Group (OMG) [37,38]. The problem with BPMN and UML modeling is that they do not include any notations or models for security requirements. BPMN models are widely used to represent business processes for the development of ERP systems. These process models help different business users understand requirements for implementing these processes. Different tools support BPMN modeling and it serves as a requirement engineering platform to understand the requirements of business analysts, users, and other stakeholders. BPMN is becoming popular because of its flexible extension mechanism for any kind of representation and the ability to extend the model for interoperability issues [39]. Furthermore, it allows using service-oriented architecture Modeling Language (SoaML) for transformation of business processes into a desired technology dependent service [40]. There are also different extensions of BPMN in which security requirements have been modeled. Most of them are theoretical and do not cover all security aspects. Some frameworks represent confidentiality, integrity, authentication, and auditability as necessary security requirements, while others consider access control mechanism as an important security requirement. Furthermore, some frameworks discuss social trust and delegation mechanisms. It must be noted that there is no framework that addresses all security requirements of an organization and their implementation. Moreover, security requirements are modeled using security goals that are too generic and are limited to information and its security. However, there are some security requirements processes that discuss the importance of security threats, but there is no BPMN extension that could represent security threats in business models.

To solve this issue, we will present our framework, which focuses on a security threat for developing security requirements and allows us to create models using the BPMN Meta model extension. We will apply this framework and extension to a business process as a case study. The framework will be useful for decision support at the conceptual level as well as for run time system changes occurring due to uncertainty and a changing environment. With the changing business requirements, the security of the system will be re-evaluated for security threats. Once the security requirements have been considered and documented in business process models, they will not be ignored during the design-time. The paper

aims at bringing together security requirement elicitation and analysis with regard to security threat concerns and, thereafter, building secure systems for performing business processes. We hypothesize that eliciting security requirements guided only by the security goals of an organization are not sufficient for comprehensive coverage of security aspects. Hence, for securing the information system for an organization, all threats must be considered. To this end, we propose:

1. A framework that will ensure systematic elicitation and analyses of security requirements in IS development.
2. A BPMN extension to model our threat-based security requirements elicitation model.
3. An application of framework with a case study for IS at the shop floor level.

The remainder of this paper is organized as follows: related work of security requirements and BPMN extensions is described in Section 2. In Section 3, the security requirements' framework and BPMN extension is presented. Section 4 describes the application of the proposed framework as a case study example and its results. Section 5 discusses the conclusion and future work.

2. Related Work

The literature has been divided into two parts. The first part shows state-of-the-art security standards and processes defining security requirements. The second part explains BPMN extensions for modeling security requirements.

2.1. Security Standards and Security Requirements Framework

The ERP system security has different dimensions, i.e., technical, human, organizational, and conformance to standards. While defining security requirements, these dimensions must be considered. ISO 17799:2005 also defines these dimensions and security controls to manage risks. It manages the informational assets like files, records, and databases [41]. ISO 27001 and its variants [42,43] are standards that are adopted by many companies that help organizations achieve credibility in a competitive market, and assure information security and risk management. They monitor, analyze, measure, and evaluate organization's information security. ISO 17799:2005, ISO 27001 deal with different aspects of information security and its assurance [41,44].

COBIT 2019 Framework [16] is an enterprise-wide governance of information and technology. The purpose of this framework is to get maximum benefits from digital transformations and mitigating business risks, which can arise due to digital transformation. This standard is applied on enterprise governance to ensure that the organizational objectives are fulfilled. It works on management of plans and activities to achieve governance objectives. COBIT defines the holistic approach for dynamic governance system, which is distinct from management and tailored to enterprise needs. This standard includes processes, services infrastructure, applications, people skills, competencies, culture, ethics, behavior, information, principles, policies, procedures, and organizational structure. Its design factors help organizations plan and acquire IT infrastructure for its operations with different scopes. Most important is the risk profile and threat landscape, which has become the motivation for our proposed framework. COBIT has arrived as a general enterprise wide applicable security information and technology standard. Comparison of all these standards is shown in Table 1.

Existing security standards can help define metrics to measure the organization's preparedness for security [44]. For this purpose, different researchers have proposed different frameworks. A threat-based approach is defined for IS in IoTs [34]. The approach is based on ISO 27005 and ISO16982. It defines an IoT infrastructure such as local environment, transportation, storage and data mining, and provision. They are further defined in terms of assets and are mapped to security goals and threats in a matrix form. The framework serves as a guideline for identification of assets and threats at different layers.

There are different database security standards [45] and guidelines [46] defined by common criteria to secure the databases. They define assets and threat agents, organizational security policies,

security objectives, security functional requirements, security audit, identification, and authentication. In Reference [47], authors propose different kinds of database threats that can occur in a database and proposed their countermeasures. There are different security objectives defined by ISO standards and these objectives can be selected on the basis of organizational requirements [41] and access control serves as a major role in attainment of these objectives. Adopting an IS does not mean that it can work autonomously until every stake holder of that system is involved and motivated about its importance and criticality [48] and requires a dynamic system to control the threats occurring at run time with a changing system's functional requirements [49]. Studies [7,32,42,44,46,50] have shown that people using the ERP are a major threat to its security, which intentionally or un-intentionally damages the security. These damages can be reduced by explaining the criticality of the security, by educating the populace, by setting accountability, or by deterrence. Every study and standard has highlighted nearly the same aspects of security such as security policies, objectives, threats, security audit of people, threat agents, network security, cryptography, physical security, disaster management, assets management, access methods, and accountability and auditability of people. There is not a single standard that defines the mechanism to design the secure IS for organizations that covers all these security aspects. There must also be a proper audit system for the security management to keep check on the suspected security issues on the whole. There is the need to model the security requirements not only related to information, but it should make the organization's system secure from physical access, natural disasters, network, operational, and at applications' level threats.

Table 1. Comparison of existing security standards.

Standard	Purpose
Common Criteria	Information technology security assurance
ISO 17799: 2005	Procedural security, physical security, human related security and technical security, assets, compliance
ISO 27001, 27k	Information security management requirements
COBIT 2019	Enterprise governance of information and technology and benchmarking

2.2. Security Requirements Modeling Using BPMN

Business Process Modeling has been widely used in designing IS. It covers business functions of an organization by modeling the interaction between different departments and processes. However, it does not provide any mechanisms to show the security requirements of these processes, which is the main concern of today's IS. There are goal-based and threat-based approaches to analyze the security requirements. The goal-based approach is an abstract approach that highlights the goals that can be achieved and includes all threats underlying the goal. While the threat-based approach is more detailed and analyses-specific threats define security requirements [51]. Different attempts made by the researchers have been summarized in Table 2, where they have introduced text annotations, constraints specification, and visual notations to show access control and limited goals to represent security requirements in the BPMN. In Reference [52], they have introduced the role-based authentication mechanism, where individuals are certified to use the system through identification and monitoring. In Reference [33], social trust based on security mechanisms have also been introduced, which are used to define trustworthy objects and delegate tasks to other people based on trust [27]. Security is insufficient without the representation of security objectives and their adherence to security requirements [52–56]. They are named goal-based security BPMN extensions and focus on security goals of information security only whose attainment defines the overall security of IS. However, comparing these extensions with each other, there are inconsistencies in definitions of security goals and security requirements. In Reference [52], authors have not discussed availability, which is the important goal defined by the ISO 2700x standard. However, its domain is service-oriented architecture, where the availability of service is an important issue. In Reference [53], authors have shown the Confidentiality, Integrity, Availability (CIA) triad as security goals, but they are applied only to pools

and use of the security task is also not defined. In Reference [33], authors have presented a broad definition of trustworthiness that includes performance, reliability, usability, and security. They have defined trustworthy goals, threats to trustworthiness, and controls to maintain the trust. Its main concern is to maintain privacy trust. In Reference [54], Salnitri et al. have proposed eight security goals that have also been defined in the information assurance reference model (IAS). These goals are mapped to activity, data objects, and connecting lines. Despite the model-only emphasis on security goals, there is no concept of security roles, secure communication, and constraints. They have covered only limited aspects of security, which are too generic. In Reference [42], Rodriguez et al. have proposed the security requirement as non-repudiation, attack harm, integrity, privacy, and access control. They have also applied security roles and permissions on privacy and access control. The approach is simple with well-defined security requirement mapping rules and security goals represented with a padlock symbol. The text annotations are used to represent access controls. The proposed model misses important security goals like availability, confidentiality, and auditability. In Reference [56], Cherdantseva et al. have proposed security requirements based on a Reference Model of Information Assurance and Security (RMIAS) model. The model is limited to the security of information aspects only and its classifications. These goal-based security analysis approaches are at abstract level and cover limited security aspects. Considering only a set of security goals inhibits security specialists from having the essential broad vision of IS security. They consider that a goal refers to an entire category of threats. Thus, the emphasis on the attainment of several pre-defined security goals, rather than on the achievement of sufficient security, is a weak approach, as it may lead to an omission of some threats. However, when we analyze the nature of threats, we find that there are different classes of threats with different complexities and have the capability to affect different security goals with different severity levels [30]. In order to make all components such as information, people, business procedures, hardware software, and networks of an IS secure, we have to define a bottom-up approach. There is a need to define specific requirements relating to each security threat and then combine them to give the holistic view of the organization's security. Until now, there is no BPMN extension that models and analyses the security threat and proposes security requirements based on security threats. There is no unified method using BPMN models that can model not only security issues of information but an organization's complete system.

Table 2. Summary of existing Secure Business Process Management Notation (BPMN) extensions.




























Paper Title	Security Requirements	Symbols/Annotation	Application Domain	Research Scope
A security language for BPMN process models [52]	Role Assignment Assignment Mechanism User Assignment Binding of duty Separation of duty Delegation Adaptation Confidentiality Authentication Auditing Integrity	Annotations specifying constraints converted into executable process	Service oriented architectures	Access control Information Security
	Security Task			
BPMN Security Extensions for Healthcare Process [53]	Authorization		Health Care system	Access Control Information Security
	Authentication			
	Access Control			
	Harm Protection			
	Encrypted Message			
	Non-Repudiation			
	Secure Communication			

Table 2. Cont.

Paper Title	Security Requirements	Symbols/Annotation	Application Domain	Research Scope
A Framework for Systematic Refinement of Trustworthiness Requirements [33]	Monitor Point		Health Care System	Access Control based on Social Trust
	Delegation of Duty			
	Trustworthy objects			
	Interaction point			
	Constraints on delegation			
	Technical Resource			
	Trustworthy Technical Resource			
Designing secure business processes with SecBPMN [54]	Accountability		Air Traffic Control Management System	Security Goals representation Verification of security goals
	Auditability			
	Authenticity			
	Availability			
	Confidentiality			
	Integrity			
	Non-Repudiation			
	Privacy			
	BPMN Query language to verify the security requirements			
A BPMN extension for the modeling of security requirements in business processes [55]	Integrity		Health sector	Limited security goals
	Attack harm detection			
	Privacy			
	Non-Repudiation			
Towards secure BPMN—Aligning BPMN with the information assurance and security domain [56]	Security role	Text annotations	Language translator	Information security assurance using security goals
	Security permissions	Text annotations		
	Information assurance security model			
	Security goals name, criticality			
	Information	Information as multi-dimension concept		

3. Proposed Methodology

3.1. Threat-Based Security Requirements Framework and BPMN Extension

We are proposing a framework based on the threat profile mechanism of an organization. Threats are more dynamic in nature and determine the severity of organizations' security by the losses they cause to the organization. A system cannot be made secure until there is a defined security policy of an organization and also that security policy is implemented in true letter and spirit. It is also required that people from top management to end users understand the criticality of security policy and adhere to it. Our proposed framework is based on Software Quality Requirements Engineering (SQAURE), which is a generic security requirement engineering model, and Software Requirements Engineering Process (SREP), which elaborates SQAURE using common criteria. Our framework defines different dimensions of threats that can be used to elicit security requirements using SQAURE. We have

also defined the structure of the security policy document based on our framework. Our framework consists of seven different steps, as shown in Figure 1. The proposed model is the combination of iterative and sequential process activities.

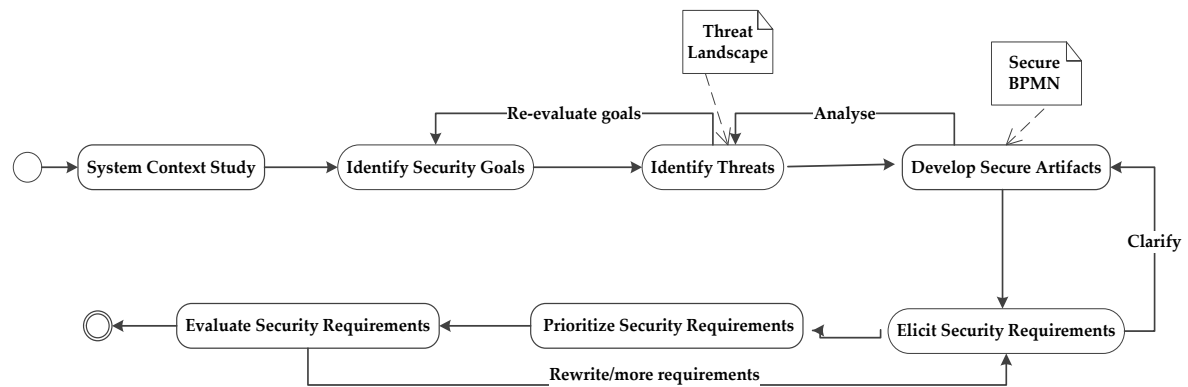


Figure 1. Security requirements framework using the threat profile technique and BPMN extension model.

3.1.1. System Context Study

SREP [19] and SQAURE [18] define this phase as agreed upon definitions, security policies, and security vision of organization. Our system context defines the background of organization, type of processes, their criticality, and what security level the organization wants to achieve. Usually, businesses prepare a vision document at the starting phase of the requirements engineering process. We will name it as a security vision document as its purpose will be the security of an organization's system that will lead us to the next stages of our framework. This document can be structured using the existing documentation standards of preparing a vision document or can be customized by the organization itself. This phase is a sequential activity, which will either be conducted at the start of the system or when the system will undergo maintenance.

3.1.2. Identify Security Goals

Security goals consists of confidentiality, integrity, availability, auditability, privacy, authenticity, or trustworthiness as well as non-repudiation and accountability for any secure system [51]. Security goals and business goals along with the management control define the overall business goals of an organization. Security goals determine the desirable properties of IS. It is necessary for a system to identify these business goals at early stages of development. Security requirements are defined as constraints to achieve these business goals. In most of the research, when security requirements are defined without security goals, they were replaced with architectural components of the system like encryption, access control, virus detection tools, and firewalls [17]. Security goals are defined as an important phase in secure requirement engineering processes [18,19] and this phase occurs at the initial stages of these processes. Therefore, we need to identify the security goals of our manufacturing system.

Due to the constant change in the environment, new threats constantly emerge and security goals are only valid for the environment at a certain stage. This occurs when any set of goals rapidly becomes incomplete in a changing landscape and some threats stay out of the scope of IS security. This situation can make the system unstable. Therefore, security goals are defined iteratively, a goal is selected, and its scope will be determined partially based on stability of the environment. Then we can proceed to the next stage of our framework.

3.1.3. Identify Threats

An IS is secure if it is protected from all the threats. Both the SQUARE and SREP define the generic techniques of elicitation, but it is better to define the elicitation technique that can elicit a maximum of security requirements in a cost-effective way. We have proposed a threat landscape model for requirement elicitation. It includes anticipated security threats and its impact on security goals. Threats to IS security are classified into insecure network services, transportation failures, insecure mobile interface, insecure firmware, poor physical security, data breach, malicious code, service abuse, identity masquerade, replay attack, routing attack, misconfiguration, excessive privileges, weak audit trail, data input injections, weak authentication mechanisms, denial of service, discarding outdated resources' bootable media containing information, limited education of personnel using systems, theft of equipment, compromise of functions, tampering with software and information, failure of IT infrastructure, unauthorized actions, geopolitical issues, acts of nature, and system usage problems, etc. [16,30,34,47]. These different kinds of threats reflect different aspects of vulnerabilities exploited by different attacking agents with different intentions and their results on companies and their systems. Threats to information systems can be categorized. Corresponding security goal and security requirements are defined for each category of threats. A set of security goals, identified as a result of a threat analysis, have to be revised from time to time to ensure its conformance with the evolving environment. Identify security goals and identify security threat phases are interlinked and re-iterate through these two phases. Identify security goals and identify security threat phases are interlinked and re-iterate through these two phases. Before proposing security requirements, it is necessary to analyze the nature of each threat from different dimensions. Therefore, we have defined four dimensions of a security, as shown in Figure 2.

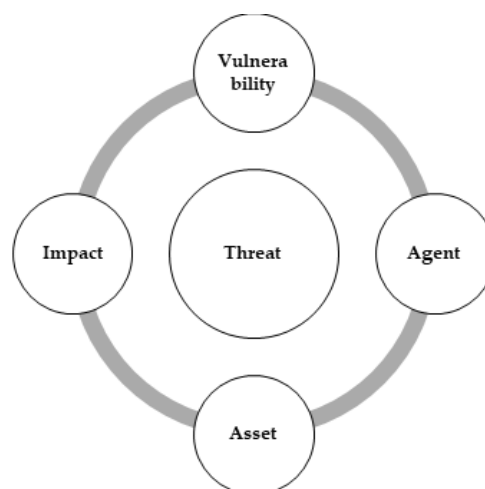


Figure 2. Proposed dimensions of a security threat.

This phase is iterative in nature. It will iterate until all the threats are identified on the basis of specific vulnerability, asset attacker, and their impact is a measurable threat can be elicited using the following four dimensions.

1. Vulnerability

The first dimension of the framework is the identification of anticipated gaps or vulnerabilities that can become an opportunity for different types of agents and can cause different security threats for an organization. Therefore, identification of vulnerabilities is an important part for anticipating security threats.

2. Agent

An attack is never self-generated. It is always created by an agent or a situation. Attacking agents are divided into five categories shown in Figure 3. Types of attacking agents for security threats in security requirements framework.

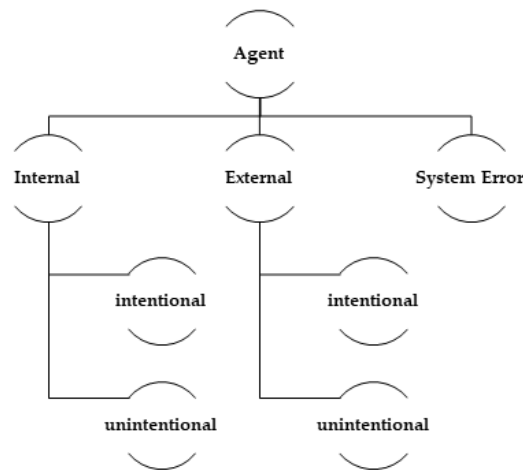


Figure 3. Types of attacking agents for security threats in security requirements framework.

An internal agent can be an employee who might generate a threat either to get some financial or operational benefit or unintentionally violates the security goals. An attacker can be external who intentionally like a hacker accesses the system for some defined purpose. An external attacker can be an unintentional supplier who does not follow supplier compliance requirements and damages the system security. There is a possibility of some system error, which is a situation that can stop the services and makes the system unavailable or performance issues can cause the financial losses to the company.

3. Identify Assets

An organization has different types of assets such as physical resources, soft resources, services, and virtual resources. Physical assets include land, building, machinery, plants, and stock, etc. Soft resources include information, patents, trademarks, and software systems. Services include network connections, third party suppliers, etc. Virtual assets include representation of currency that can be exchanged at different levels. It is important to identify the assets and their criticality to the organization for estimating the impact of attacks and their countermeasures.

4. Threat Impact

According to COBIT, the threat impact determines the risk of an organization in an environment [16]. When an asset is subject to a security threat, it affects our security goals. This effect is called impact and is measured as low impact or high impact on security goals. It is like a risk assessment to find out whether a company is operating in a low threat environment or a high threat environment. If the impact of attack on a goal is high, the whole manufacturing system can be compromised. Impact of threat on the goal is defined as either low impact or high impact.

3.1.4. Develop Secure Artifacts

In this phase, we will represent our threat-based elicitation technique using BPMN extension. Expressing the threat profile framework using visual notations captures the attention of business personnel and developers. Therefore, it helps them address pitfalls highlighted at early stages of development. In this phase, threats will be analyzed iteratively and modeled using BPMN extension until a consolidated list of threats is defined to fulfill the whole scope of our security.

1. BPMN Extension Mechanism

The BPMN standard has defined an extension mechanism to add artifacts or elements, according to the specific needs of modelers. An extension contains four parts: extension, extension definition, extension attribute definition, and extension attribute value [37]. The extension definition and extension attribute definition are core extension elements. The extension definition can be any BPMN or non-BPMN element and extension attribute defines the name and type of attribute. This extension must not conflict with the existing elements of the BPMN standard. We have shown our secure BPMN meta model extension is in Figure 4. We have shown extended security objects are shown with shaded rectangles.

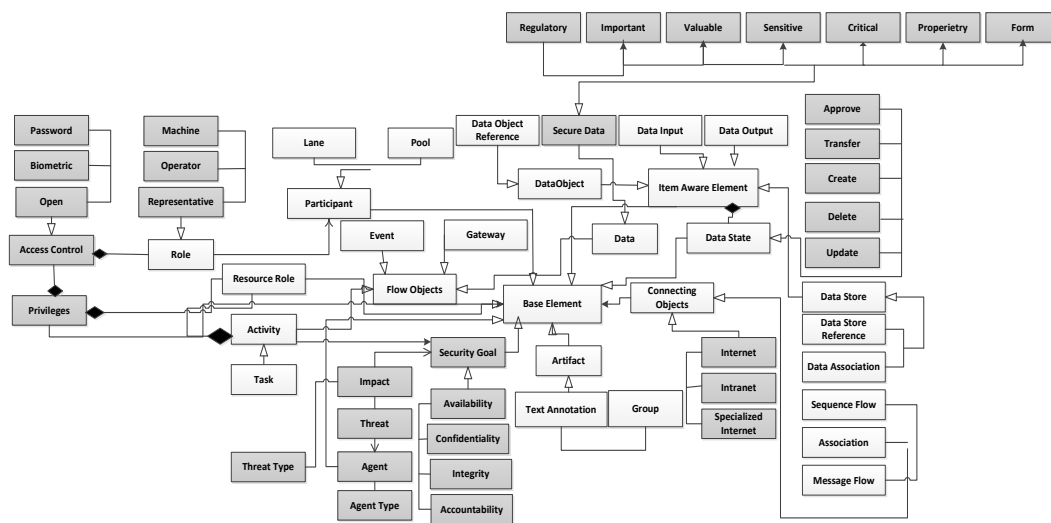


Figure 4. Proposed BPMN meta model extension using security objects.

2. Secure BPMN extension objects and their attributes

We have defined the security goal, secure data type, threat, access mechanism, privileges, and transfer ways as extended BPMN object definitions. The security goal has attributes of name, ID, and threat impact. Data object is defined using ISO 27,001 along with additional classes of documents. The attributes of data objects can be a type such as regulatory, important, sensitive, critical, and proprietary and form. A form is added as it is most often referred in manufacturing and has a defined format. Other attributes of data objects are state and transfer mechanism. Threat object contains the attributes' threat name, ID, agent, and impact, which is connected with the goal. Attributes of the access mechanism are defined using three types of access methods such as password, biometric, and open. Privilege object defines the access of processed tasks, activities, and resources. This access can be created, updated, deleted, read, written, or transferred of an object. Transfer attribute contains the attribute of the type of transfer mechanisms. Resource instances are fixed by specifying resource instances to match the organizational assets.

3. Visual Representation of Extended Objects

All the extended objects and their attributes are defined using visual notation. Icons of goal and threat impact are represented using the notations. Data has different states such as approve, transfer, create, update, and delete. They are defined in BPMN 2.0.2 but did not have any visual notations. In order to define the security requirements for IS, it is necessary to make these states visible. Therefore, we have represented these data states using a marker on the BPMN data object, as shown in Figure 5.

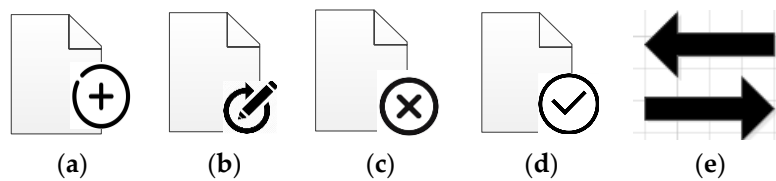


Figure 5. Different states of the document object using a BPMN extension. (a) create, (b) update, (c) delete, (d) approve, (e) transfer.

ISO 27001 defines sensitive, critical, and valuable types of data that determine the nature and criticality of information and needs to be secure accordingly. We have defined additional data types such as proprietary, important, regulatory, and form. These types are represented using the notations shown in Figure 6.



Figure 6. Visual representation of different types of data objects in the BPMN extension. (a) critical, (b) important, (c) propriety, (d) regulatory, (e) sensitive, (f) form, (g) valuable.

Classification of the document helps in ensuring the saving and transfer of documents, according to their level of security. A sensitive document needs to be transferred more securely than an important document. We will use a padlock symbol along with the connections to show a secure transfer of critical and sensitive documents.

Security roles are added, and privileges are assigned to use the resources to create a task or change its state. Privileges are assigned to activities and tasks. In this case, privilege is defined as a flag to represent grant and revoke objects to roles. Threats are classified in different types. Each type of a threat is assigned a graphical representation. Stencils for threat instances is created and security requirements are defined using text. The combination of a goal and a nature of threat determines the security requirements. The goal and threat impact are modeled using icons shown in Figure 7.

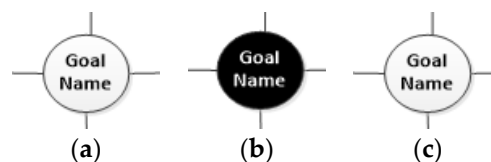


Figure 7. Visual representation of security goal and impact of threat on goal in the BPMN extension. (a) security goal symbol, (b) high threat of impact on goal, (c) low impact of threat on goal.

4. Representation Rules in BPMN 2.0.2

Representation rules of all these extended objects and attributes are mentioned in Table 3. The objects are represented using separate icons and data states are represented as markers on the right bottom corner of data objects. The access mechanism is represented using an icon at the pool, data object, and resource. Communication icons are positioned at the connecting objects.

Table 3. Attributes of extended security objects in BPMN.

Object Name	Attributes	Representation
Goals	Name	Marker
Threat	Threat name	Marker
	Threat impact	Marker
	Threat agent	Position
Data Object	Regulatory	Icon
	Important	Icon
	Valuable	Icon
	Sensitive	Icon
	Critical	Icon
	Proprietary	Icon
	Form	Icon
Data State	Create	Marker
	Update	Marker
	Delete	Marker
	Approve	Marker
	Transfer	Marker
Access Mechanism	Open	Position
	Password	Position
	Biometric	Position
Communication	Internet	Position
	Intranet	Position
	Specialized Internet	Position

Threats also have certain attributes, which need definition and mapping rules. The threat has attributes of name, impact, and agent, which causes that threat. The threat name and threat impact are represented as a marker while the threat agent is represented at the top of the threat icon.

Agents of five different types are represented by icons and are shown in Figure 8. These icons are placed on the top right corner of the threat.



Figure 8. Visual representation of attacking agents and situations in the BPMN extension. (a) un-intentional external agent, (b) Intentional external agent, (c) System error, (d) Un-intentional internal agent, (e) Intentional internal agent.

Table 4 shows the mapping between the existing BPMN elements and threat profile objects. The goal can be used in connection with pool, activity, task, connecting objects, data objects, and resource and message flow and the goal cannot be applied to a data state.

The access mechanism is applied to the pool, data object, and a resource. Communication is applied to only connecting objects. Access privileges are applied to the pool, activity, task, data object, data state, and a resource.

Table 4. Mapping of extended security objects with basic elements of BPMN.

	Pool	Activity	Task	Connecting Object	Data Object	Data State	Resource
Goal	✓	✓	✓	✓	✓		✓
Threat	✓		✓	✓	✓	✓	✓
Access mechanism	✓				✓		✓
Communication				✓			
Security requirement	✓	✓	✓	✓	✓	✓	✓
Access privileges	✓	✓	✓		✓	✓	✓

3.1.5. Security Requirements Elicitation and Evaluation

Security requirements are defined on the basis of threat impact on assets and violation of security goals. Security requirements will determine the extent to which a specific threat can be avoided or tolerated. Security requirements are defined in a natural language. A goal may map to multiple security requirements based on the category of the threat. Hence, it is necessary to prioritize these requirements according to their criticality, cost of implementation, and benefit to the organization. The security requirement will be evaluated using the requirements' verification and validation techniques. This phase is also iterative, as it will move through different reviews of security requirements and updates. At the completion of this phase, the security requirements' document will be ready to merge with the Requirements Engineering (RE) process.

4. Case Study

We have demonstrated our framework and its BPMN model with a case study taken from aircrafts' manufacturing company at the shop floor level. In this example, the process of workshop 1 is modeled. The process starts with the reception of materials and job card from the production department. Job card includes the product design and instructions for the manufacturing of the product and its parts. The business process model includes the dispatcher of workshop 1, storekeeper, concerned Incharge bay, worker, and QC Incharge (QCI). The dispatcher of workshop 1 transfers the work package along with required documents to the store keeper. Which transfers the package to a concerned bay, where the suitable workers are deployed and provided with required materials and tools. The task of the worker is to design the product and send it to QCI for quality inspection. QCI send the designed product along with documents to the store keeper after performing an inspection and the store keeper calls the dispatcher of the production department to hand over the completed task. The whole process is manual and it involves people and lots of manual entries on registers. The process has been shown in Figure 9.

Security requirements' development framework consists of the following steps for the above example.

Step 1: System context study

We will start with the system context study. The manufacturing organization is a big industry and security of its processes and systems is very critical to it. This phase helps in determining overall security goals and security requirements of the organization.

Step 2: Identify Security Goals

Manufacturing organizations have a closed environment where every role is defined and the process is fixed. Every event occurs according to a schedule, which is also called a production schedule. Therefore, the availability of the production systems and resources is important. Companies may not want to share their proprietary information with any other system or people until they are authorized to use it. Confidentiality is also considered an important security goal. Organizations have their product

designs or maps. If any change in design occurs, it can change the whole product, and its integrity is an important goal. Since the system will be used by many people designated at different roles, there is a need to add accountability acts and people must be educated about it. Therefore, four security goals: integrity, confidentiality, availability, and auditability are most important for the security of the manufacturing organization. These goals determine the overall security objectives of the organization and are shown in Figure 10.

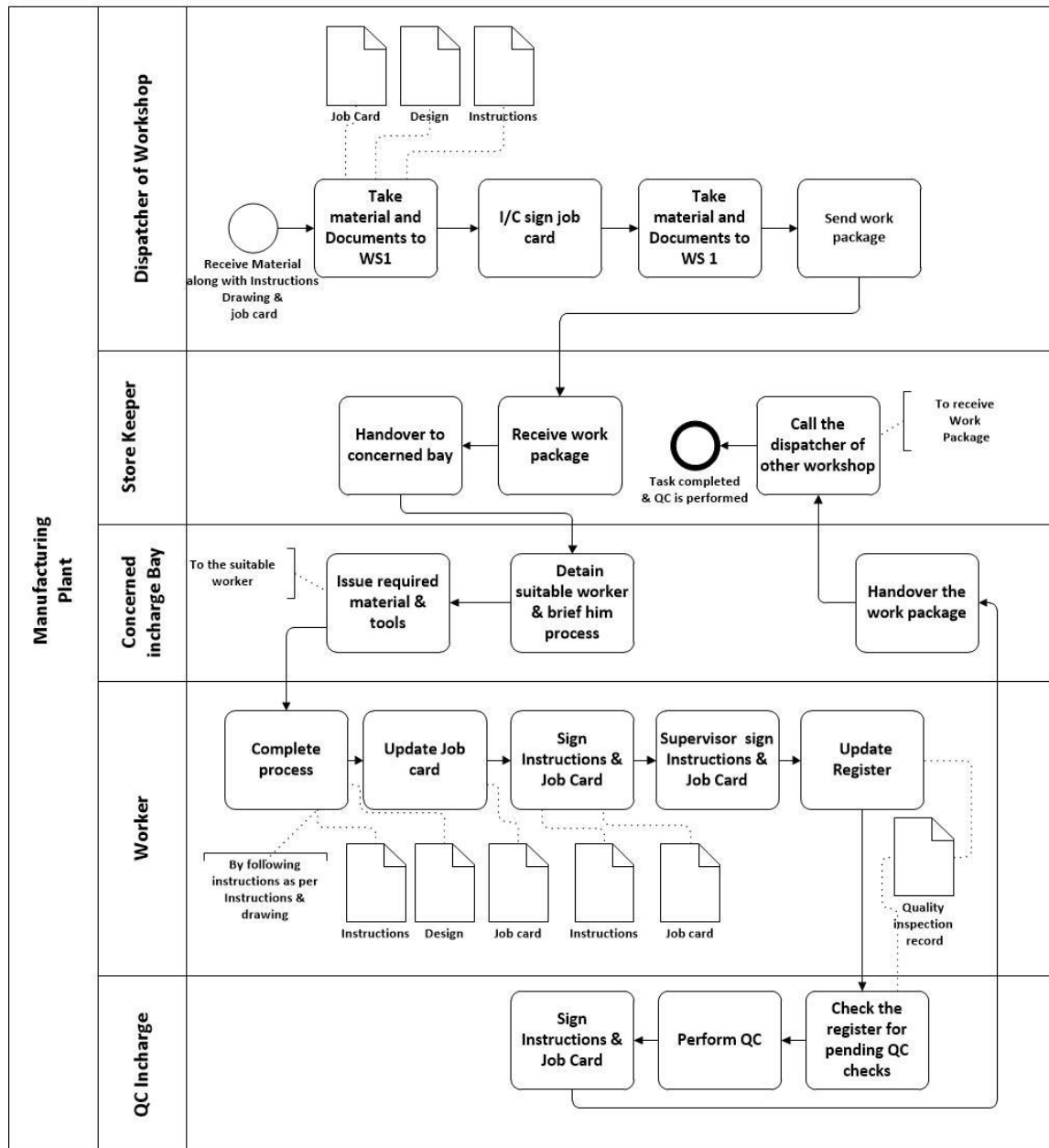


Figure 9. BPMN example of receiving a task from Workshop 1 and handing it to the concerned bay.

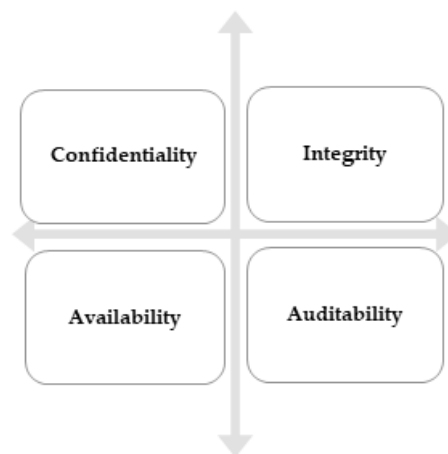


Figure 10. Selected security goals for a manufacturing organization.

Steps 3–4: Identify Threats and Develop Secure Artifacts

The next phase is the identification of threats to its processes, documents, and assets and modeled using BPMN 2.0.2. In this example, dispatcher, QC Incharge, worker, and storekeeper are identified as security roles that must seek permission before starting any work. Security roles are mapped to the accountability goal. These roles can cause the threats' elevation of privileges, non-compliance to their job description, and malicious activities using their accounts. These threats are due to an intentional internal attacker and can cause more damage to the company. Therefore, their impact on the accountability goal is mapped as high impact.

There are many security aspects in each lane. In the dispatcher workshop 1 lane, different types of documents are mentioned. All these documents are of different types and criticality. There are some materials that are required and need to be taken care, as mishandling of these materials can cause delays and problems in the manufacturing process. Then, the activities represent different states of these documents such as transfer, approval, and transfer to another lane. In transferring the document to another lane, the documents must be securely transferred based on the nature of their classification. If a document is normal, it can be transferred using the normal transfer mechanism. Therefore, resources can also be optimized in a cost-effective way. Assets such as materials, machinery, and tools, and documents are received by the storekeeper, who transfers them along with required resources to the Incharge bay. These assets are mapped to the availability goal.

The storekeeper has no privileges to read or modify or delete the documents. His task is to just transfer the package. The Incharge bay has the privileges to read the documents and assign the additional resources such as required labor and materials. Availability of raw material and required tools is very important along with their design instructions and schedule. Else production can be delayed. It has been mapped with denial of service threat and its impact has been shown as high.

Labor includes people who are less educated and physical access restriction of labor into the premises is enough. However, labor is accountable to follow the standards of the item production process. The worker is accountable not to leak the design and patent details outside the premises through any intellectual way or mobile media. Labor completes the production process and updates the status of the job card by signing it. It transfers the item and all documents to the supervisor. He adds details in the database and sends the item along with instructions as a complete package to the QC inspector (QCI).

QCI perform the inspection process and sends the item to the Incharge bay who, in turn, gives it to the storekeeper, where the work package is handed over to the dispatcher. During this process, the intentional internal attacker can gain the physical access to a manufactured work package and can damage its integrity with high impact on the goal. These security threats are applied using graphical notations on the case study, as shown in Figure 11.

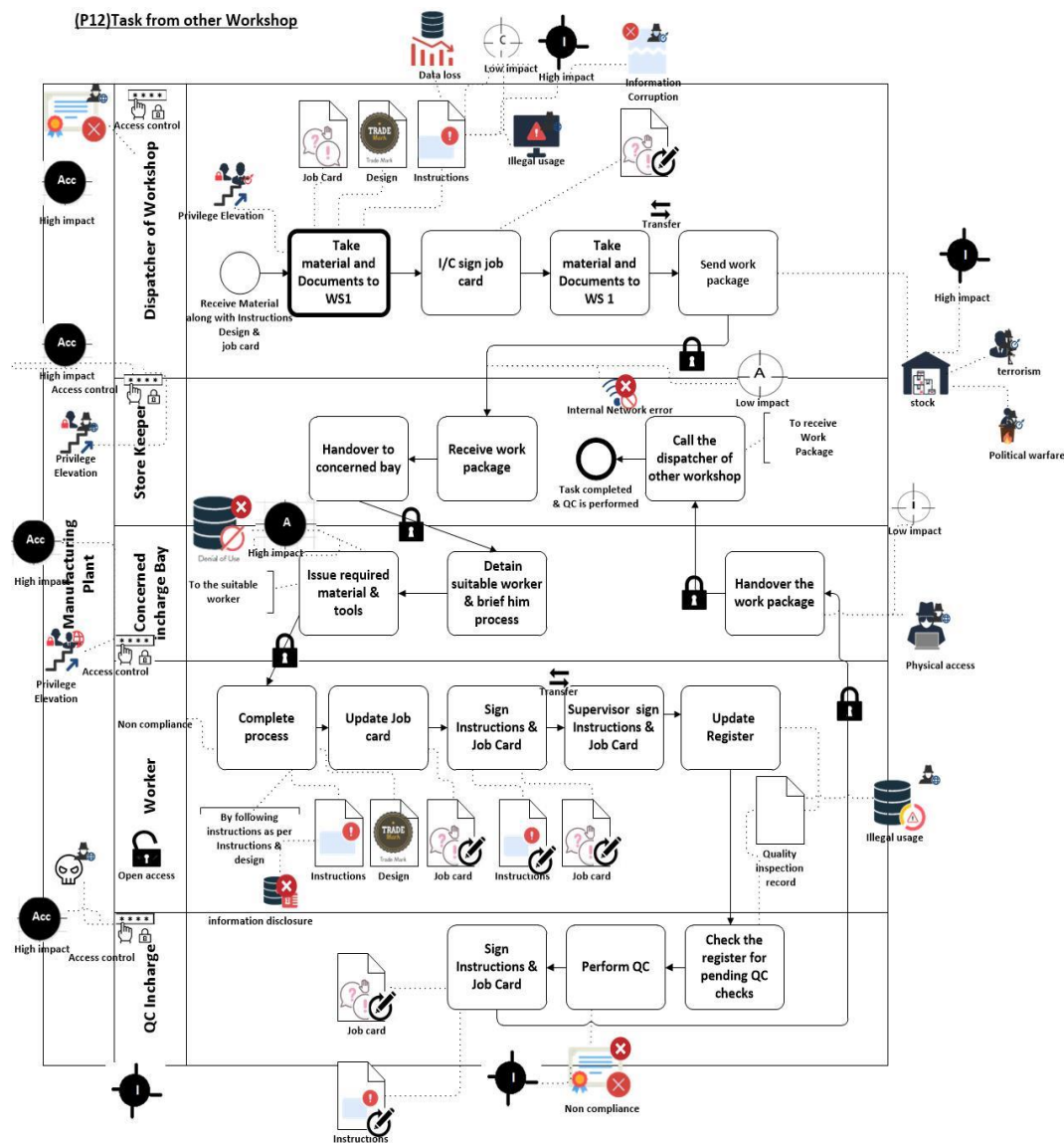


Figure 11. Receiving task from the other workshop and handing it to concerned bay using the proposed Business Process Management Notation (BPMN) extension.

Storage of an item is shown as a stock asset and that asset can be subject to intentional external agent attacks such as terrorism and political warfare that can have a high impact on the integrity of the organization. Natural disasters such as fire, floods, earthquakes, etc. can cause damage to integrity due to the organization's inability to prepare itself against them and its agent is considered as a system error. After secure BPMN mapping of each threat landscape, security requirements are defined, and this step can be repeated to clarify the concepts.

Step 5: Requirements Elicitation and Evaluation

The next phases are requirements' prioritization and their evaluation. According to Table 5, there are more than one security requirement against each threat, so it will be decided by the stakeholders, that requirements are feasible to implement and which requirements are more important. After that, the requirements' statements should be evaluated using the requirements' writing guidelines, which are measurable, unambiguous, and consistent requirements.

Table 5. Elicited security requirements along with risk analysis using threat-based security requirements framework.

Goal	Risk Profile	Threat Landscape			Security Requirements
		Threat	Attacker/Problem	Impact	
Confidentiality	1. Data and information management incidents (regulatory, critical, sensitive, important, valuable, form) 2. Data flow/migration	1. Unauthorized access to storage media 2. Internal network failure 3. External network failure	Unintentional Internal attack	Low	System access shall be given to the authorized user. Information shall be restricted according to its type. Critical and sensitive information shall be transferred using the secure communication. A user is authorized by the job role she performs. System shall have a granular access mechanism. In case of open access for workers, resources and activities shall be defined. (Principal of least access privilege). The system shall monitor privileged users such as storekeeper, dispatcher, and concerned Incharge bay for not changing the state of data. The system shall define the alternative path of information transfer. The system shall restrict the use of unauthorized bootable, shortcut keys, and storage media.
		4. Theft/loss of information	Intentional internal	High	The security policy of information use shall be clearly communicated to employees. The accountability process shall be established by logging each user's actions. For external attacks, the system shall be able to monitor the external traffic and user's behavior using log files.
			Intentional external attacks	High	
		5. Disclosure of information	Intentional internal and external attacks	High	The security policy of the manufacturing system shall be shared with the employees. Information shall be transferred according to different categories so that the user cannot get complete information. The accountability process shall be established.
		6. Illegal usage	Intentional internal attack	High	The system shall monitor the activity of each user by logging each event in a log file.
			Intentional External Natural external phenomena	High	System must have a backup plan located at a different place from the manufacturing industry. The system shall be able to take backup at regular intervals of time. The system shall have the control mechanism to shut down itself properly before any invasion or security alarm.
Integrity	1. Geopolitical issues 2. Environmental 3. Governance issues 4. Regulatory issues 5. Supplier quality process 6. Document control mechanism	1. Destruction of information 2. Political warfare 3. Terrorism 4. Illegal access 5. Noncompliance of standards 6. Corruption of information 7. Logical attacks 8. Dataflow/migration 9. Timing synchronization	Intentional External	High	Regular audit system shall be placed to identify the non-compliance. Regular backup of information shall be implemented. The system shall disable auto run facilities to any user terminal. Communication with outside users shall be conducted securely using Virtual Private Networks. The firewall shall be implemented to restrict incoming communication. A dedicated operating system shall be used to restrict the users.
			Intentional external attacks	High	Documents transfer shall be restricted according to their sensitivity. No role shall be able to create and approve the same document. System shall ensure secure storage of data on disks from unauthorized people. Security of data marts shall be ensured using encryption and secure key management. Each activity in the system shall be controlled by its timing schedule.

Table 5. Cont.

Goal	Risk Profile	Threat Landscape			Security Requirements
		Threat	Attacker/Problem	Impact	
Availability	1. Low productivity 2. Industrial action 3. Information handling error 4. Service error 5. Internet protocols 6. Shared networks 7. Operational IT incidents	1. Software usage problem	Internal User Problem	High	Users of the system shall be trained to use the software. The system shall introduce a mechanism to report a flaw or problem to the development team.
		2. Infrastructure failure	Unintentional internal	High	Alternative path shall be defined for smooth running of tasks.
		3. Machine failure			
		4. Network failure			
		5. Infrastructure overload	Unintentional internal	High	System shall notify about infrastructure overload.
		6. Software failure	Unintentional internal	High	System shall shut down after notifying about the error.
		7. Data inconsistency	Indirect cause to a threat	Low	System shall apply a mechanism for input and output validation.
		8. Poor data quality	Internal system problem	Low	System shall implement well-defined data definitions.
		9. Data access problems	Internal user problem	Low	Users shall be given open access to a minimum set of resources. System shall be able to log the errors.
		10. Hardware incidents	Unintentional internal	High	System shall report the specific error to the administrator and stop the services.
		11. Removal			
		12. Maintenance			
		13. Media error			
Accountability	1. Noncompliance with the given security policy	14. Denial of use	Intentional external attacks Intentional internal attack	High	The system shall restrict on multiple concurrent sessions. The system shall monitor for common attack types for internal and external traffic. System shall monitor the activities of employees by logging their activities.
		1. Elevation of privilege/increased access	Intentional internal attack	High	The system shall restrict employee from creating and approving any task.
		2. Malicious activity	Intentional external/intentional internal	High	System shall monitor for malicious activities by logging user id, time, and events.

5. Discussion

The example shows that it is possible to show goals and threats together in the BPMN model. Both goals and threats give a broader view about the security of aspects of workflow model in BPMN. Using a goal threat-based approach set of security requirements can be defined as cluster of security requirements cluster and these clusters can be applied whenever the same goal threats are encountered. It also requires that, during every iteration of the goal, threat, and risk analysis using the BPMN extension, every change must be tracked and saved for future reference. Therefore, a repository needs to be developed using available software configuration management applications. The defined system model is not separate from the required engineering process, or does not replace the required engineering process. It needs to be integrated with the required engineering process to ensure the importance and place of security requirements and to fit in the overall system's requirements.

Comparing the security requirements framework with SQUARE and SREP shown in Table 6, SQUARE is a generic process that refers to elicitation and specification of quality requirements in which security is the one kind of non-functional requirement. It ignores the consideration of assets that are referred to by most of the security standards and approaches of security engineering. It does not have a defined method of security requirements and risk analysis. On the other hand, it suggests that threat tree and misuse cases can be used for this purpose. SQUARE is also supported with a tool.

Table 6. Comparison of security requirements engineering process phases.

Phases							
Security Requirements Engineering Process	Assets	Vulnerabilities	Threats Model	Risk Analysis Techniques	Security Requirements Specification	Validation	Tool Support
SQUARE	No	No	Suggest Misuse cases and attack trees	Yes	Yes	Yes	Yes
SREP	Yes	Partially	Suggest UMLSec, Misuse cases, and attack trees	Yes	Yes	Yes	No
Security Requirements Engineering Framework	Yes	Yes	Defined Threat-based business process models	Yes	Yes	Yes	Yes

Considering the SREP framework, it defines the concept of protection profiles and packages based on a common criteria standard, but its example and application is not found regarding defined packages and protection profiles. The standard defines the abstract concepts of protection profiles and packages and does not give systematic support for use in security requirement definitions. SREP considers the concept of assets or vulnerabilities interchangeably. It considers them as the same thing and it does not have any tool for application of the framework.

Extended BPMN is compared with BPMN standard 2.0.2 and BPMN extension using Reference Model of Information Assurance (RMIAS) in Table 7. The BPMN standard is developed to facilitate communication between stakeholders. BPMN is rich in syntax and allows us to model the business processes in different scenarios. BPMN does not include any graphical notations for security objects like security goals, threats, attacking agent assets, their states, security roles, and access mechanisms. However, BPMN has defined text annotation that can be used to show user defined concepts during process modeling. BPMN has defined data object that can be used to represent information assets only. The last column of the table shows another extension proposed based on RMIAS. It moves around the information and considers the security goal, which refers to an entire category of threats. Security goals are more abstract in nature and cannot reflect all anticipated threats as threats are becoming more complex and have the capability to affect different security goals with a different impact. Our extension considers the goal and threats that are necessary to model in order to secure IS and the organization itself and considers all assets of organization should be considered important in which information is one. Their record is also kept in IS along with the information generated and processed in the organization.

Table 7. Comparison of proposed BPMN security objects with BPMN 2.0.2 and Reference Model of Information Assurance (RMIAS) model.

Proposed Security Objects in Threat Base BPMN Extension	Visual Representation in BPMN 2.0.2	BPMN Extension Using RMIAS
Security goal	Not present	Present
Attack	Not present	Not present
Attacking agent	Not present	Not present
Asset	Data object	Information only
Asset state	Not present	Information state
Security roles	Not present	Not present
Access mechanism	Not Present	Not present

However, the BPMN model will become cluttered with security objects and notations. It can distract business modelers from the flow of the main process. Therefore, we suggest to add security notations after the process flow is discussed and finalized with the stakeholders. The concept of granting and revoking privilege can be shown as an abstract notation as flags. We cannot show details such as which roles have privileges through visual notations. These are constraints that can be defined using other methods.

6. Conclusions and Future Work

Security of IS has become an important issue and requires attention at early phases of system development. Since security is not only limited to information, instead, the entire process of the manufacturing system should be guaranteed to be secure. BPMN provides a flexible mechanism that enables us to model security requirements along with business process models. While security threats are encountered at different levels such as processes, storage, and communication and at the physical level of an organization. Herein, we presented a threat-based security framework and its BPMN extension to model the security threat that helps in risk analysis and define security requirements of organizations. This would facilitate the uses of this representation and negotiate the security aspects of a business with different stakeholders of the system. The model is implemented when using a case study of an aircraft's manufacturing organization, which is going to adapt an ERP system to automate its organizational processes and is concerned about security. Our results show that the proposed threat profile covers a broad range of security requirements considering all assets rather than information only. A goal-based approach shows the abstract concepts and goals are subject to change whenever the environment of an organization changes. The threat-goal approach is useful to elicit security requirements in changing environments such as if the organization wants to evolve with the changing climate such as smart manufacturing or Industry 4.0 paradigms.

In the future, we will further refine the approach to show the classification of threats on the basis of the architecture of the software model that covers different aspects of the organization. A detailed evaluation of the proposed model will be carried out by involving different industries and users of the system. Moreover, the model will be evaluated to find out if the security requirements are covered for manufacturing the system based on the layered architecture of ERP systems.

Author Contributions: S.Z. conceptualized and prepared the original draft. A.A. and S.A.K. supervised and reviewed the draft. All authors have read and agreed to the submitted version of the manuscript.

Funding: This research received no funding.

Acknowledgments: We thank Asjad Saleem for improving English Language and Madiha Liaqat for comments that greatly improved the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ehie, I.C.; Madsen, M. Identifying critical issues in enterprise resource planning (ERP) implementation. *Comput. Ind.* **2005**, *56*, 545–557. [\[CrossRef\]](#)
2. Han, S.W. ERP—Enterprise Resource Planning: A Cost-Based Business Case and Implementation Assessment. *Hum. Factors Ergon. Manuf. Serv. Ind.* **2004**, *14*, 239–256. [\[CrossRef\]](#)
3. Klotz, B. The central and eastern European online library (www.cceol.com). *Ser. Libr.* **2007**, *53*, 191–201. [\[CrossRef\]](#)
4. Dospinescu, O. Mobile Payments. from Mobility to Security. *Young Econ.* **2012**, *5*, 190–193.
5. Erturk, E.; Arora, J.K. An Exploratory Study on the Implementation and Adoption of ERP Solutions for Businesses. *Int. J. Sci. Tech. Res.* **2017**, *8*, 1092–1097.
6. Ma, Z.; Hudic, A.; Shaaban, A.; Plosz, S. Security viewpoint in a reference architecture model for cyber-physical production systems. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017; pp. 153–159. [\[CrossRef\]](#)
7. Marnewick, C. Labuschagne a Security Framework for an Erp System. *Indian J. Comput. Sci. Eng.* **2008**, *3*, 548–552.
8. She, W.; Thuraisingham, B. Security for enterprise resource planning systems. *Inf. Syst. Secur.* **2007**, *16*, 152–163. [\[CrossRef\]](#)
9. Bu, W.; Xue, M.; Xu, L.; Zhou, Y.; Tang, Z.; Xie, T. When program analysis meets mobile security: An industrial study of misusing android internet sockets. In Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, Paderborn, Germany, 4–8 September 2017; pp. 842–847. [\[CrossRef\]](#)
10. Pascu, C. Security Principles in ERP Systems 2. ERP Systems Security 3. Oracle E-Business Suite Three-Tier Architecture. *J. Mob. Embed. Distrib. Syst.* **2013**, *5*, 36–44.
11. Koo, J.; Oh, S.R.; Lee, S.H.; Kim, Y.G. Security architecture for cloud-based command and control system in IoT environment. *Appl. Sci.* **2020**, *10*, 1035. [\[CrossRef\]](#)
12. Häckel, B.; Hänsch, F.; Hertel, M.; Übelhör, J. Assessing IT availability risks in smart factory networks. *Bus. Res.* **2019**, *12*, 523–558. [\[CrossRef\]](#)
13. ISO 27001 Information Technology-Security Techniques-Information Security Management Systems-Requirements; ISO/IEC International Standards Organization, Schweitzer Norm: Winterthur, Switzerland, 2013; Volume 2014, p. 38.
14. Quinn, S.D.; Cook, M.; Cook, M. National Checklist Program for IT Products—Guidelines for Checklist Users and Developers. *J. Res. Natl. Inst. Stand. Technol.* **2018**, *4*, 1–52.
15. Common Criteria Implementation Board. Common criteria for information technology security evaluation part 1: Introduction and general model. *Common Criteria* **2017**, *3*, 1–106.
16. Isaca. *COBIT2019 Framework Introduction and Methodology*; ISACA: Schaumburg, IL, USA, 2019; ISBN 9781604207637.
17. Salini, P.; Kanmani, S. Survey and analysis on security requirements engineering. *Comput. Electr. Eng.* **2012**, *38*, 1785–1797. [\[CrossRef\]](#)
18. Mead, N.R.; Stehney, T. Security Quality Requirements Engineering (SQUARE)Methodology. *ACM Sigsoft Softw. Eng. Notes* **2005**, *30*, 1–7. [\[CrossRef\]](#)
19. Mellado, D.; Fernández-Medina, E.; Piattini, M. A common criteria based security requirements engineering process for the development of secure information systems. *Comput. Stand. Interfaces* **2007**, *29*, 244–253. [\[CrossRef\]](#)
20. Bresciani, P.; Giorgini, P.; Giunchiglia, F.; Mylopoulos, J.; Perini, A. Tropos: An Agent-Oriented Software Development Methodology. *Auton. Agent. Multi. Agent. Syst.* **2002**, *8*, 203–236. [\[CrossRef\]](#)
21. Mouratidis, H.; Giorgini, P.; Manson, G. When security meets software engineering: A case of modelling secure information systems. *Inf. Syst.* **2005**, *30*, 609–629. [\[CrossRef\]](#)
22. Dardenne, A.; Van Lamsweerde, A.; Fickas, S. Goal-directed requirements acquisition. *Sci. Comput. Program.* **1993**, *20*, 3–50. [\[CrossRef\]](#)
23. Sindre, G.; Opdahl, A.L. Eliciting security requirements with misuse cases. *Requir. Eng.* **2005**, *10*, 34–44. [\[CrossRef\]](#)
24. Jürjens, J. *Secure Systems Development with UML*; Springer: Berlin/Heidelberg, Germany, 2005; ISBN 978-3-540-26494-1.

25. Hong, S.; Park, S.; Park, L.W.; Jeon, M.; Chang, H. An analysis of security systems for electronic information for establishing secure internet of things environments: Focusing on research trends in the security field in South Korea. *Future Gener. Comput. Syst.* **2018**, *82*, 769–782. [CrossRef]
26. Gatchin, Y.A.; Sukhostat, V.V. Research of Vulnerabilities of Information Processing Processes Systems of Critical Information Infrastructure. In Proceedings of the 2019 Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 3–7 June 2019; pp. 1–4.
27. Bitton, R.; Finkelshtein, A.; Sidi, L.; Puzis, R.; Rokach, L.; Shabtai, A. Taxonomy of mobile users' security awareness. *Comput. Secur.* **2018**, *73*, 266–293. [CrossRef]
28. Abdelrazek, M.; Grundy, J.; Ibrahim, A. Adaptive Security for Software Systems. In *Managing Trade-Offs in Adaptable Software Architectures*; Morgan Kaufmann Burlington: Burlington, MA, USA, 2016; pp. 99–127, ISBN 9780128028551.
29. UK Essays The Threats Of Information System Security Information Technology Essay. *Inf. Tech.* 2016. 4964706. Available online: <https://www.ukessays.com/essays/information-technology/the-threats-of-information-system-security-information-technology-essay.php?vref=1> (accessed on 17 July 2020).
30. Li, S.; Tryfonas, T.; Li, H. The Internet of Things: A security point of view. *Internet Res.* **2016**, *26*, 337–359. [CrossRef]
31. Kraus, K. Security Management Process in Distributed, Large Scale High Performance Systems. *Online J. Power Energy Eng.* **2010**, *2*, 228–247.
32. Sindre, G.; Firesmith, D.G.; Opdahl, A.L. A Reuse-Based Approach To Determining Security Requirements. In Proceedings of the 9th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03), Klagenfurt/Velden, Austria, 16–17 June 2003; pp. 127–136.
33. Mohammadi, N.G.; Heisel, M. A framework for systematic refinement of trustworthiness requirements. *Information* **2017**, *8*, 46. [CrossRef]
34. Dorsemayne, B.; Gaulier, J.P.; Wary, J.P.; Kheir, N.; Urien, P. A New Threat Assessment Method for Integrating an IoT Infrastructure in an Information System. In Proceedings of the 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, USA, 5–8 June 2017; pp. 105–112. [CrossRef]
35. Michael, M. Physical Security Threats and Measures. In *Handbook of Computer Networks*; Wiley: Hoboken, NJ, USA, 2007; Volume 3, pp. 596–631. ISBN 9780471784609.
36. Al-Sayid, N.A.; Aldlaeen, D. Database security threats: A survey study. In Proceedings of the 2013 5th International Conference on Computer Science and Information Technology, Amman, Jordania, 27–28 March 2013; pp. 60–64.
37. Aagesen, G.; Krogstie, J. Bpmn 2.0 for modeling business processes. In *Handbook on Business Process Management 1: Introduction, Methods, and Information Systems*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 219–250. ISBN 9783642451003.
38. OMG Object Management Group. Business process modeling notation (BPMN) version 2.0.2. *Object Manag. Gr.* **2013**, *134*, 429–453. [CrossRef]
39. Heguy, X.; Zacharewicz, G.; Ducq, Y.; Tazi, S.; Vallespir, B. A Performance Measurement Extension for BPMN. In *Enterprise Interoperability VIII*; Popplewell, K., Thoben, K.D., Knothe, T., Poler, R., Eds.; Springer: Cham, Switzerland, 2019.
40. Dospinescu, O.; Strimbei, C.; Strainu, R.-M.; Nistor, A. REST SOA Orchestration and BPM Platforms. *Inf. Econ.* **2017**, *21*, 30–42. [CrossRef]
41. Qingxiong, M.; Johnston, A.C.; Pearson, J.M. Information security management objectives and practices: A parsimonious framework. *Inf. Manag. Comput. Secur.* **2008**, *16*, 251–270. [CrossRef]
42. Disterer, G. ISO / IEC 27000, 27001 and 27002 for Information Security Management. *Int. J. Inf. Secur.* **2013**, *2013*, 92–100. [CrossRef]
43. Ioanna, T.; Maria, K. From theory to practice: Guidelines for enhancing information security management. *Inf. Comput. Secur.* **2019**, *27*, 326–342. [CrossRef]
44. Tashi, I.; Ghernaouti-Hélie, S. Security metrics to improve information security management. In Proceedings of the 6th Annual Security Conference, Las Vegas, NV, USA, 11–12 April 2007.
45. Common Criteria Development Boards, U.S. Government. *Base Protection Profile for Database Management Systems*; 2015; BSI-CC-PP-0088. Available online: https://www.commoncriteriaportal.org/files/ppfiles/pp0088b_pdf.pdf (accessed on 17 July 2020).

46. Consortium security guideline WG, D.S. *Database Security Guideline*, version 2; 2009, pp. 1–41. Available online: http://www.db-security.org/report/dbsec_guideline_ver2.0_e.pdf (accessed on 17 July 2020).
47. Pevnev, V.; Kapchynskyi, S. Database Security: Threats and Preventive Measures. *Adv. Inf. Syst.* **2018**, *2*, 69–72. [CrossRef]
48. Katua, F.S. Information Security Management Strategy Implementation Challenges at Kenya Electricity Generating Company. Ph.D. Thesis, University of Nairobi, Nairobi, Kenya, 2014.
49. Jahan, S.; Riley, I.; Walter, C.; Gamble, R.F.; Pasco, M.; McKinley, P.K.; Cheng, B.H.C. MAPE-K/MAPE-SAC: An interaction framework for adaptive systems with security assurance cases. *Future Gener. Comput. Syst.* **2020**, *109*, 197–209. [CrossRef]
50. Safa, N.S.; Maple, C.; Furnell, S.; Azad, M.A.; Perera, C.; Dabbagh, M.; Sookhak, M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Gener. Comput. Syst.* **2019**, *97*, 587–597. [CrossRef]
51. Cherdantseva, Y. Secure* BPMN—a Graphical Extension for BPMN 2.0 Based on a Reference Model of Information Assurance & Security. Ph.D. Thesis, Cardiff University, Wales, UK, 2014. Available online: <http://orca.cf.ac.uk/74432/> (accessed on 1 June 2020).
52. Mülle, J.; Von Stackelberg, S.; Böhm, K. *Security Language for BPMN Process Models*; A Security Language for BPMN Process Models; Karlsruhe Reports in Informatics 2011,9. Karlsruhe Institute of Technology, Faculty of Informatics ISSN 2190-4782. Available online: <https://pdfs.semanticscholar.org/ad1b/e8bcb0bcdf1abded15fb674fe27df56232f5.pdf> (accessed on 20 June 2020).
53. Sang, K.S.; Zhou, B. BPMN security extensions for healthcare process. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications, Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 27–28 October 2015; pp. 2340–2345. [CrossRef]
54. Salnitri, M.; Dalpiaz, F.; Giorgini, P. Designing secure business processes with SecBPMN. *Softw. Syst. Model.* **2017**, *16*, 737–757. [CrossRef]
55. Rodríguez, A.; Fernández-Medina, E.; Piattini, M. A BPMN extension for the modeling of security requirements in business processes. *IEICE Trans. Inf. Syst.* **2007**, 745–752. [CrossRef]
56. Cherdantseva, Y.; Hilton, J.; Rana, O. Towards SecureBPMN—Aligning BPMN with the information assurance and security domain. In *Lecture Notes in Business Information Processing*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 125, pp. 107–115.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).