Chapter 5

Business Procedures and its Capabilities

The essence of this chapter is to provide an idea of procedure adopted during any business transaction specifically e-business. The definition of ‘business process’, together with a discussion of the various components of such a process in a modern organisation is discussed to know exactly what the business process is. Since we have adopted a business process-oriented approach, giving a definition of a business process is an essential prerequisite for the development of our security model. The detailed discussion of the term we provide in this chapter will motivate certain key decisions relating to the components of the security model.

5.1 Defining the Process

Management and operation are the two fundamental components of any organisation. Management cares for Planning and control [209]. The operations component is the most basic but essential without operations there is no management, and hence there is no organisation. No organisation can function as an active unit without performing its processes. Running of an organizational processes are mandatory to ensure the functionality of that organization. The term ‘Business Process’ discussed widely. -see for example [82,157,178,227]. The vast majority of prior discussions do not give a formal definition for a business process, and the few that do provide a variety of definitions. Lindsay et al. [11] argue that the existing definitions of business process are limited in depth, and that the business process models are, therefore, constrained. There are also a number of points of view from which business processes can be described and defined, and various ways of specifying them. We now review some of these definitions.

A business process can also be defined as a sequence of activities that transforms inputs from suppliers into outputs to selected customers, consider inputs that are turned into outputs by using a transformation process. Such definitions treat a business process as a set of logically related business activities that combine to deliver some kind of value. So a process, as commonly defined, is a conversion/transformation of a certain entity, tangible or non-tangible from one form to another, while undergoing a series of actions. Hence, from a purely business point of view, a business process is a means of achieving a commercial result and as such, it can be defined as a collection of inputs, decisions, activities and outputs. According to Forbus [138], the ways in which things change are intuitively characterised as processes'. The author also asserts that our description of the world has been static, and although we can say that things are different from one time to another, we have not described the means by which changes actually occur. Processes, says the author, are the analogy of differential equations, used to describe the dynamics of the system. Based on his
perception that a physical process is something that acts through time to change the parameters of objects in situation, Forbus [138] suggests specifying processes using the following elements: individuals, a set of preconditions, a set of quantity conditions, a set of relations and a set of influences. These elements appear useful when dealing with processes from an operational point of view.

Business process design and management are not covered by any of the definitions discussed above. In order to execute a business process, the interaction between the operational features has to be designed and managed, i.e. the business logic has to be in place. In order to provide a comprehensive organisational framework to deal with processes, covering both operational and management perspectives, and also including business logic, and to build a set of business processes characteristics, the following process characteristics should be considered:

- The purpose of a process
- How the purpose is to be achieved
- How a specific process should be integrated with other processes within a specific organisation;
- Who is in charge of the development and/or maintenance of a specific process?

The process characteristics should include both the Forbus criteria and the list of process properties given above. Business logic defines the functionality of all the elements of a process during its execution and the relationships between them. It deals with the performance of business-related tasks [288], that is what resource, when, where, for how long and by whom should be used in order to produce a product, service, idea or decision. Building on the purpose of a process (i.e. management aspect), it defines the process operational parameters (i.e. how and by which means the process is executed). That is, business logic defines both the process specification elements of Forbus [138] and management (namely, planning and control) elements of Anthony [209]. Business logic can be expressed in terms of business rules [288], which are reflected in business procedures and policies. These can be designed in more than one way, the optimal design being one that gives a rational and efficient way of running a specific process, that effectively coordinates the process elements. The following definition of a business process is thus suggested as a working definition for the purposes of this thesis: a business process is a sequence of decisions and actions that are rationally coordinated and directed according to specific business logic, influencing some of the process elements and meeting one of the strategic or tactical goals of the business. Since there is an output for each business process, there is always a user at the end of the process, i.e. an employee, customer, or another process.
Therefore, the definition includes both operational aspects such as inputs, outputs, actions, and means of performing a process as well as management aspects such as design and management in terms of business purpose, business integration and coordination, resource allocation, and control. Generic process definition explained above is not complete. Because with advances in information technology and the subsequent changes in the business environment, business processes have also gone through certain modifications. In a modern business environment, many organisations are able to leverage critical business operations through Internet-based electronic processes [24]. Specifically, the business processes in an e-business organisation have certain unique features and properties. In order to achieve the goal of this chapter, i.e. to provide a definition of an e-process, the main differences between traditional processes and e-processes are next considered.

5.2 Conventional business Vs e-business process characteristics

Any process related to the business is performed either by people or by technological means, or a combination of both. The outputs are employed by users (customers, employees) or by another process, while the interface between a process and its users can be either technological or human. In traditional processes, associated with traditional types of business, the level of human participation in a process is greater than the technological, and/or the technology itself is not specifically information technology. The more the organisation practices more modern modes of running a business, the greater the proportion of information technological involvement in processes. Moreover, a traditional type of organisation will perform its processes within the organisation's boundaries.

The e-business mode of doing business implies that business processes associated with that e-business are performed by means of Information Technology only (or at least mainly) and across the organisational environment, both inside and outside the organisation's boundaries. Hence, any business process can be classified into one of the following three types:

- **A conventional process:**
  - Performed by people and technology/tools;
  - The human involvement is greater than that of technology;
  - The technology and the tools are mostly non-Information Technology based;
  - Performed within the organisation's boundaries;
  - Inputs and outputs are physical.

- **A modern process:**
  - Performed by people and technology/tools;
  - The technology component is relatively large compared to the human part;
The technology and tools mostly involve Information Technology (computer hardware, software, databases, LANs);

An intra organisational process—it is performed within the organisation's boundaries;

Inputs and outputs are physical and/or digital.

An e-business process:

- The technology component is significantly larger than the human component;
- Inputs and outputs are digital (data and information flows);
- There are no logical or physical organisational boundaries, just the process and its route;
- Inter organisational - the process is performed both inside the organisation and between organisations;
- An inter organisational process, an e-business process might also be performed between organisations from different countries;
- Different process components go through different business environments, and are subject to differing business requirements, policies, mechanisms and concepts (along with differing security concepts and policies).

Building on these characteristics of the various process types, and the differences between them, we can now define an e-business process (e-process).

5.3 E-business processes

Establishment of a business whether it is a conventional business process or an e-business process involving two or more business partners. E-business process could be realised by composing Web services offered by the individual business partners [77]. However, irrespective of the process type, any process is a part of an organisation's value chain. Following the value chain concept [95,167] discussed in chapter 3, a value chain is made up of a streaming set of activities, namely processes. These activities consume information and also generate information. To make the information generated by an activity available to subsequent activities, data links are needed [77]. These data links exist in the form of information flows. An e-business process is characterised by the fact that it is performed electronically; its component tasks are information and data flows, and its outcomes are specific pieces of information. These outcomes could be a product, service, idea or decision, or be associated with one or more of the outcome types mentioned above. An e-business process is performed solely using Information Technology. According to Wang et al. [181], e-business processes are high-level computing processes built upon and supported by lower-level computing and networking services. In other words, e-business organisation processes are completely automated using Information Technology, and are executed according to a strictly defined business
logic. Hence a generic e-business process is performed between parties that do not necessarily know (or are not sure about) the details of the entity with which they are exchanging information. In systems analysis, processes are activities performed in the system and are described using systems analysis tools, such as DFDs (Data Flow Diagrams), structured English, etc. [161]. A business process, from this perspective, entails transforming documents between stations involved in a specific series of actions in order to complete a specific mission. Documents contain data essential to perform each of the stages of a process. In other words, the contents of the documents and the procedures reflect the business logic, while the documents are used as a convenient way of carrying data. Hence, a process can be described in terms of the documents carrying data relevant to the process.

Dynamic organisation is a characteristic of a modern business, not only to do the processes change, but also the relationships between the processes and even the channels used to execute the processes. Smith and Fingar [93] distinguish three characteristics of a modern business process:

- **State** - The value of calculations performed, and the information collected and generated during execution of the process;
- **Capability** - The joint activities and relationships established between the participants during the process;
- **Design** - The intentional characteristics of the process, specified during its design.

Building on the above discussion of the dynamic characteristics of a process, the following working definition of an e-business process is proposed: an e-business process is a predefined set of information flows regulated by certain states and capabilities, creating a valuable output according to a particular design, which is dictated by specific business logic. The various information flow contents, destinations, and their sequence in a specific e-process, are completely defined by the business goals, which are expressed by the business logic. Two types of information flow can be distinguished: those associated with a specific business action required by business logic such as obtaining the details of an ordered item and those associated with the implementation of the operation using Information Technology such as the sequence of bits making up an operation. These two types of flow will be referred to here as BRIFs (Business-Related Information Flows) and SRIFs (System-Related Information Flows), respectively. In this thesis, the role and operation of the two types of information flows fit the state characteristics of Smith and Fingar [93] discussed above, whereas the capabilities are represented here by the various process participants, or Process Agents, which are discussed in section 5.4 below. The design is made in accordance with the business logic of an e-process.
E-business security can be defined in terms of the security of its e-processes. The primary hypothesis underlying the security model developed in this thesis is that a ‘secure e-business’ is achieved when the correctness of its e-processes is ensured. Hence, we need to consider e-process security requirements. The following two aspects of an e-business process need to be considered:

- The business logic;
- The actual information flows by means of which the e-process is executed, including the SRIFs and the BRIFs.

E-process protection should start with careful design and implementation [181]. E-process correctness cannot be achieved by relying solely on technology solutions [283], even though we may assume perfect protection from firewalls, IDSs, IPSs, strong confidentiality protection from unbreakable encryption schemes, etc. Leymann et al. [77] focus on the relation between Web services and business processes, as well as on the elements required for a suitable standard. They describe specific security incidents resulting not just from technical failures, but also from a lack of input control over product Web catalogues. The problem was not related to technical security or reliability, but in basic e-process design [77]. The authors emphasise the fundamental importance of secure and reliable e-processes. E-process correctness is inherently a multilayered problem [181].

5.4 E-business process agents

The e-process elements can be secured by ensuring that they are designed, developed, executed, and maintained appropriately by the relevant entities that interact with the e-process elements. We call these entities process agents. There are four types of legitimate participant, or process agent, in an e-business process:

- The e-business organisation (the organisation practicing the e-business mode of doing business, i.e. the main owner of the e-business process.
- Other organisations involved in the process under discussion.
- The customers of the e-business organisation.
- The ISP providing Internet services to the e-business organisation.

Each of these participants has security requirements related to the e-business mode of doing business. We need to consider whether there are differences in security requirements between these four classes of participant, arising from the differences in their status in the e-process. The e-business organisation that develops and owns the e-process is interested in correct process performance and execution, namely that the correct business logic is being executed between the correct users at the correct times with the correct contents and via the correct channels. The e-business organisation gives access to the e-process, and enables authorised interactions between the e-process and employees such as back office employees, remote workers, salesmen, system
developers, network operators and administrators, system administrators) and other participants in the execution of the e-process organisations, customers, ISPs.

The other organisations that have business relations with the e-business organisation have the same requirements as the e-business organisation itself. They will also be concerned that the e-process under discussion is able to integrate with their own e-processes that need to interact with it. They will further be concerned that the e-process is compliant with their own security requirements and policies. The customer is a person whose motivation to enter the e-business organisation portal is for the purposes of purchasing or viewing company products and services needs to know that his/her personal information will stay confidential, will reach the intended destination, and that it will be possible for them to perform transactions at the times that they wish namely that the channels and the portal of the organisation are accessible and usable.

The ISP, i.e. a company that provides the e-business organisation, its partners and its customers with access to the e-business company's portal over the Internet, and that hosts the company website [190], is concerned with the reliability and availability of its service, and that the connection between the ISP and the e-business company will not be used for the purposes of violating or compromising the ISP infrastructure or its other clients. Apart from the four classes of legitimate participant outlined above, external individuals or organisations may wish to gain unauthorised access to the e-process. An Intruder is a person or organisation whose motivation to enter the e-business organisation portal is for any kind of activity that will violate the security requirements for the e-business organisation's information systems. Intruders can act in order to gain strategic business, commercial or financial information about an organisation i.e. net espionage activities, or to deliberately cause damage to an organisation. An Intruder is treated here as a illegitimate process agent. The legitimate participants might also violate the e-business security requirements, intentionally or accidentally. Intentional violations could be facilitated by their access to, and knowledge of, the characteristics of an e-process in a specific business environment. Building on the analysis of the two case studies, and also on personal experience, we divide these five classes of Process Agent (PA) into the following more detailed classes of participants, according to their role in an organisation e-process. The classification includes the following types of PA.

- Executives,
- System developers,
- System administrators,
- Network administrators,
- Back Office employees (including clerical staff, remote workers and salesmen),
- Participant organisation employees,
Customers,
Intruders,
ISPs.

This list of PA categories may not be exhaustive. In practice, an analysis will need to be performed to produce a version of this list tailored to the specific e-business organisation.

5.5 Summary

In this chapter the nature of a business process has been discussed and defined. First the concept was introduced, and then, based on that definition, an e-business process was defined. Also, a comparison between traditional and e-processes was provided, emphasising the differences between them. The relationship between an e-business and the correct execution of its constituent e-processes has been discussed. The main conclusion of this discussion is that e-business information security can be approached by analysing the security of the constituent e-processes.

As discussed above, in section 5.3, e-processes are composed of two elements, namely business logic and information flows. Business logic is built according to the business and operational requirements. A detailed discussion of business logic, in the context of this thesis, is provided in chapter 8. The term `information flows' in this thesis is assigned a meaning which differs from the meaning usually implied in computer science. In order to explain and illustrate the meaning of the term in this thesis context, the information flows component is discussed in the next chapter.