# Chapter IX
# A Roadmap for Delivering Trustworthy IT Processes

**Kassem Saleh**
*American University of Sharjah, UAE*

**Imran Zualkernan**
*American University of Sharjah, UAE*

**Ibrahim Al Kattan**
*American University of Sharjah, UAE*

## ABSTRACT

*Due to the proliferations of computers and networks, organizations are providing many of their services online. Consequently, organizations are becoming more vulnerable to attacks by cyber criminals, in addition to attacks by insiders. Ultimately, these attacks lead to reducing the trust in the organization and the trustworthiness of its provided services. Online services are mainly provided using internal IT processes. In this chapter, we provide a systematic roadmap that addresses the delivery of trustworthy IT processes at the strategic, tactical and operational levels. This roadmap is based on a defensive and preventive approach to ensure the trustworthiness of the services provided by an organization. We argue that to deliver trustworthy services, the IT processes used must be trustworthy themselves. The requirements for implementing and delivering trustworthy IT processes in an organization are discussed. For each IT process, we discuss how confidentiality, integrity, availability, accountability, reliability, privacy and business integrity requirements can be satisfied.*

## INTRODUCTION

The proliferation of computers and networks and the need to provide network-based online services is making organizations more vulnerable to attacks by malicious users, among which are cyber terrorists and cyber criminals. In this chapter, we propose a defensive and preventive countermeasure approach against cyber terrorism and cyber warfare that can be adopted by organizations. Information technology (IT)

departments within such organizations are responsible for the delivery of trustworthy IT services, and consequently, fending off malicious users and attackers. IT services are delivered through the execution of processes at the strategic, tactical, and operational levels. Our proposed approach relies on ensuring that these IT processes are themselves trustworthy. In this chapter, we first refine Microsoft's definition of trustworthiness (Mundie, deVries, Haynes, & Corwine, 2002) and refine the 38 IT processes identified by Luftman (2003). Then, we discuss how each of the refined trustworthiness requirements, which obviously includes security requirements (Firesmith, 2003), can be considered in the engineering and management of each of the refined IT processes. The result of this chapter can be used as a generic roadmap to achieve trustworthiness in delivering IT processes. Organizations of different sizes and different IT budgets can adapt and use this generic roadmap for their own situations. This roadmap can also be extended and used for the qualitative and quantitative assessment of service trustworthiness.

The rest of this chapter is organized as follows. First, we provide some preliminary background on trustworthiness and IT processes, and their refinements. Then we will provide an introduction to defensive measures against cyber attacks and the need to embed security and trust in the way we engineer and manage IT systems. Next we present the generic requirements for trustworthiness of IT processes at the strategic, tactical and operational levels. We conclude by providing some ideas for further investigation.

## BACKGROUND

Trust in IT-based systems is a topic of current interest among researchers and practitioners. Delivering high assurance and trustworthy services has been subject to long-term initiatives by Microsoft,Cisco, the Software Engineering Institute (SEI), among others (Mundie et al., 2002). According to Microsoft, the four pillars of trustworthy computing are security, privacy, reliability, and business integrity. Security addresses issues related to confidentiality, integrity, availability, and accountability. Privacy is related to the fair handling of information. Reliability is related to the dependability of the system to offer its services. Finally, business integrity is related to the responsiveness and ethical responsibility of the service provider.

Luftman identifies 38 IT processes and categorizes them into three layers (Luftman, 2003). First, the strategic layer consists of three processes focusing on the long-term goals and objectives of the organization and considering the strategic alignment of IT and business objectives. These three processes are: business strategic planning, architecture scanning and definition, and IT strategic planning and control. Second, the tactical layer consists of 14 processes focusing on medium-term goals contributing to the strategic goals. Finally, the operational layer consisting of 21 processes providing guidance for day-to-day activities contributing to the tactical processes. Many of the tactical and operational processes can be clustered together since they can be dealt with similarly when considering their trustworthiness requirements. We have clustered the tactical processes into: IT financial management, IT human resource management, IT project management, IT systems development and maintenance, and finally, IT service engineering and management. Figure 1 shows the three layers of Luftman's IT processes.

Next we refine the four pillars of Microsoft's trustworthy computing by adapting them to trustworthy processes and trustworthy services:

- **Security:** Service clients expect that the provided services are protected from malicious attacks on their confidentiality (C), integrity (I), and availability (AV). Confidentiality implies that all data, information and knowledge are kept in confidence. Integrity means that data, information, and knowledge will only be shared with and provided to entities that are allowed to have access to it according to organizational rules. Finally, availability means that the service is available when required. At the strategic level, for example, confidentiality implies that