59

Information Technology Management Frameworks: An Overview and Research Directions

59.1 Introduction

Information technology (IT) plays a key transformational role at various levels of our lives and society. There are probably very few organizations on the planet that do not have some form of IT and/or IT-enabled organizational processes or routines. Research has repeatedly shown the positive impacts of IT on outcomes at various levels of analysis: country, society, organization, community, and individual (Banker et al. 2011; Brynjolfsson and Hitt 1996; McAfee and Brynjolfsson 2008; Venkatesh et al. 2010). For instance, Dewan and Kramerer (2000) found significant positive impacts of IT on the GDP (Gross Domestic Product) of developed countries. Recent research has found positive influence of IT on organizational outcomes (e.g., Mithas et al. 2011, 2012). In the practitioner literature, although challenges related to the management of IT function have been highlighted (e.g., Heller 2009; Luftman and Ben-Zvi 2011; Wailgum 2009), it is generally well acknowledged that IT has a positive influence on an organization and its members (McAfee and Brynjolfsson 2008; Peppard and Ward 2005). Notwithstanding such general agreements about the favorable role of IT, organizations constantly face challenges related to the effective and efficient management of IT functions for long-term, sustainable organizational benefits.

Challenges associated with managing IT functions were first recognized by organizations in the 1980s when they were concerned about the quality and consistency of services they were getting from their IT units (Arraj 2010; Whittleston 2012). In the 1990s and 2000s, organizations continued to face...
challenges related to IT management as they attempted to justify and recoup the significant investments they had made for IT. Senior executives had started to question the business value of IT and impacts of IT on organizational productivity and other key performance indicators (KPIs; Brynjolfsson 1993; IT Governance Institute 2003). During this time, academic research reported a phenomenon widely known as the IT productivity paradox that captured the notion that despite high investments in IT, organizations failed to realize any measurable benefits from these investments (Brynjolfsson 1993; Brynjolfsson and Hitt 1996). Although later research, particularly at the organizational level, has shown positive impacts of IT on organizational outcomes, it has underscored the importance of effective and efficient management of IT function in organizations (Aral and Weill 2007; Dewan et al. 2007; Dos Santos et al. 2012).

As IT becomes an integral part of today’s organizations and the IT landscape—the assemblage of IT-related infrastructure, systems, processes, and service components—becomes increasingly more complex, organizations face continuous challenges related to how their IT landscape should be managed and governed so that they are able to leverage their IT capabilities to achieve organizational goals. IT management frameworks—a set of best practice-based industry frameworks to manage various facets of organizational IT—have received widespread acceptance by organizations that attempt to manage the complexity of IT landscape and mitigate associated challenges. The diffusion and the widespread popularity of these frameworks have also been catalyzed by the changing operating environment of organizations (Ross et al. 2006). For instance, organizations have started facing intense local and global competition in recent years, and they have wanted to find ways to gain operational efficiency and strategic advantage. Further, organizations are affected by the changes in society and the world caused by the emergence and widespread diffusion of transformational technologies, such as social media and mobile technologies, and significant shifts in global political and economic landscapes. Many organizations are now able to expand their operations in countries that were not accessible even in 1980s. These organizations now face challenges associated with global distribution of resources and distributed execution of processes. Consequently, it has become imperative for such organizations to find ways to achieve and sustain operational efficiency and other organizational goals. Effective management of IT has been touted as one of the key ways to achieve such efficiency and organizational goals.

This chapter provides an overview of IT management frameworks with a particular focus on frameworks that support three specific IT management areas: (a) IT governance, (b) IT service, and (c) IT security. We briefly discuss the underlying principles and processes of these frameworks. In particular, we highlight the richness that these frameworks offer with respect to managing IT provisions, processes, activities, resources, and metrics to help organizations achieve their organizational goals. In addition to providing an overview of these frameworks, we also discuss the impacts of these frameworks on IT management practices using examples of organizations that gain by implementing these frameworks and associated practices. Finally, we offer a set of research directions that can leverage the richness of these frameworks. We focus on future research that, we believe, will have significant implications for theory and practice related to IT management. To our knowledge, this chapter is a first attempt to reduce the gap between IT management practices and research by offering a prognosis of current practice and calling for actionable future research.

59.2 Emergence of IT Management Frameworks

Although IT management frameworks have been around since the 1980s, the popularity of these frameworks among senior IT and business executives has increased in the late 1990s and early 2000s as many organizations started receiving benefits from implementing these frameworks. In recent years, organizations that develop and promote these frameworks have released updated versions of these frameworks in order to keep up with the complexity of today’s organizational contexts and operating environments. Further, some of these frameworks have received recognition from international standards bodies such as the International Organization for Standardization (ISO) and the United Nations (Zhang and Chulkov 2011). Although IT management frameworks can be
Information Technology Management Frameworks

Table 59.1 Overview of IT Management Frameworks

<table>
<thead>
<tr>
<th>IT Management Frameworks</th>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT governance frameworks</td>
<td>Frameworks that help organizations define and manage leadership and organizational structures and processes to ensure that the organization's IT sustains and extends the organization's strategies and objectives (IT Governance Institute 2003)</td>
<td>• COBIT (Control Objectives for Information and Related Technology)*</td>
</tr>
<tr>
<td>IT service management (ITSM) frameworks</td>
<td>Frameworks that help organizations ensure that the IT services are aligned to the business needs and actively support them (Cartlidge et al. 2007)</td>
<td>• ITIL (Information Technology Infrastructure Library)b</td>
</tr>
<tr>
<td>Information security management (ISM) framework</td>
<td>Frameworks that offer best practice recommendations on information security management, risks, and control within the context of an overall information security management system (ISMS) that defines a set of policies related to IT security and risks (IT Governance Institute 2008a)</td>
<td>• ISO 20000</td>
</tr>
<tr>
<td>IT project management frameworks</td>
<td>Frameworks that provide standardized methodology, guidelines, rules, and characteristics for IT project management (Project Management Institute 2012)</td>
<td>• PMBOK (Project Management Body of Knowledge)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PRINCE2 (Projects in Control Environments 2)</td>
</tr>
</tbody>
</table>

* COBIT is a registered trademark of ISACA and ITGI (IT Governance Institute).

b ITIL is a registered trademark of the Office of the Government Commerce in the United Kingdom and other countries.


classified and grouped in many different ways, we broadly classify them into four categories in keeping with the core objective(s) of these frameworks: (a) IT governance frameworks, (b) IT service management (ITSM) frameworks, (c) information security management (ISM) frameworks, and (d) IT project management frameworks. It is important to note that some of these frameworks have provisions and processes that conceptually and operationally overlap with that of the other frameworks. For example, it is possible that frameworks that are primarily developed and implemented for IT governance purposes can have provisions and processes related to ITSM and vice versa. Similarly, ITSM frameworks may have provisions and processes related to ISM. Nonetheless, we use this broad classification to categorize these frameworks because it offers a useful organizing principle for the task. Table 59.1 provides a brief overview of these four types of frameworks and examples.

IT governance is a process of specifying the decision rights (i.e., who holds the rights to make IT-related decisions) and accountability (i.e., who is held responsible for an organization’s decision-making about IT assets) to encourage desirable behavior in using IT (Weill and Ross 2004). An IT governance framework helps an organization direct and control the current and future IT endeavors. Such a framework also helps an organization meet high-level IT goals such as alignment of IT with the business, realization of promised benefits, use of IT to exploit opportunities and maximize benefits, responsible use of IT resources, and appropriate management of IT-related risks (IT Governance Institute 2003). Consistent with the practitioner literature associated with the widely used IT governance frameworks and prior academic research on IT governance, we suggest that IT governance should be an inseparable component of corporate governance and a core responsibility of the board of directors and senior executives (IT Governance Institute 2003; Ross and Weill 2002; Sambamurthy and Zmud 1999; Weill and Ross 2004; Zhang and Chulkov 2011). It should not be an isolated discipline or activity performed by the IT leadership. Instead, it should be an integral part of corporate governance and should be considered a core competence of an organization (Agarwal and Sambamurthy 2002; Jewer and McKay 2012; Willcocks et al. 2006). In a nutshell, an IT
governance framework offers a set of principles, processes, activities, and measures that help organizations develop and sustain IT governance-related core competencies and outcomes.

The underlying driver of ITSM frameworks is the recognition that IT services are crucial, strategic organizational assets. Consequently, organizations must invest appropriate levels of resources into the support, delivery, and management of these critical assets and the IT systems that underpin these assets (Cartlidge et al. 2007; Gacenga et al. 2010; Kneller 2010; Whittleston 2012). The primary objective of ITSM is to ensure that IT services are aligned to the organizational needs and actively support them. ITSM can be defined in various ways—(a) as a practice related to planning, designing, developing, delivering, and optimizing IT services, (b) as a discipline that offers processes, methods, activities, measures, functions, and roles that are needed to deliver IT services, and (c) as a profession that defines a set of skills needed to deliver high-quality IT services (Kneller 2010; Rai and Sambamurthy 2006). An ITSM framework ensures that effective implementation, management, and support of IT services, that is, IT processes, systems, and resources, will lead to organizational effectiveness in at least two ways: (a) by reducing business disruptions, loss of productive hours, and costs, and (b) by increasing revenue, improving public relations, and achieving its core objectives (Cartlidge et al. 2007). An ITSM framework offers an extensive body of knowledge, capabilities, skills, and best practices for providing value to customers in the form of IT services (Cartlidge et al. 2007; Kneller 2010; Whittleston 2012). It is intended to provide a wide range of benefits to an organization, such as increased satisfaction with IT services, improved service availability, financial savings, strategic advantage, and improved decision-making (Cartlidge et al. 2007; Gacenga et al. 2010; Kneller 2010; Whittleston 2012).

Benefits from effective IT governance practices and service management do not come without risks (Chen et al. 2011; Kouns and Minoli 2010; Spears and Barki 2010). An IT risk is a potential exposure facing an organization as a result of any aspect of the IT environment—that is, IT assets, resources, organization, or processes (Westerman and Hunter 2007). There are numerous examples of IT risks and associated adversarial outcomes faced by today’s organizations. In fact, there is hardly an organization that has not faced some type of challenges associated with IT risks such as system failure, network outage, and security breaches. Organizational IT risks can be broadly grouped into four dimensions (Westerman and Hunter 2007): availability (i.e., keeping existing processes running and recovering from interruptions), access (i.e., ensuring that authorized people have access to information and facilities they need), accuracy (i.e., providing accurate, timely, and complete information), and agility (i.e., implementing new strategic initiatives). Although IT risks are primarily related to issues connected to IT systems and people (e.g., employees), prior research has found that these risks do not necessarily arise from technical and/or people issues. These risks typically arise from high-level organizational factors, such as ineffective IT governance, uncontrolled complexity in the IT landscape, and inattention to IT-related risks (Westerman and Hunter 2007). These factors clearly indicate a need for a framework and/or standard practices to manage and control IT risks. An ISM framework is intended to provide an organization a mechanism for effective management and control of IT risks. An ISM framework is also expected to help an organization manage all aspects of IT risks through a set of processes, skills, and best practices. In conjunction with managing and controlling IT risks, an ISM framework ensures the confidentiality, integrity, and availability of an organization’s assets, information, data, and IT services (Clinch 2009; Kouns and Minoli 2010).

In the remainder of this section, we discuss three widely used IT management frameworks: (a) COBIT, an IT governance framework, (b) ITIL, an ITSM framework, and (c) ISO/IEC 27000, a family of information security standards. In keeping with the core objective of this chapter to focus on frameworks to manage IT functions in organizations, we do not discuss IT project management frameworks because IT projects do not necessarily represent ongoing activities or functions of an IT organization.

59.2.1 IT Governance Framework: COBIT

COBIT is one of the most widely implemented IT governance frameworks. It was developed in 1996 by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute.
COBIT 5 is based on five core principles (Figure 59.1). These principles dictate the processes and metrics that define the core structure of the framework. COBIT 5 is a value-driven framework that offers a comprehensive goals cascade linking the framework with a set of organizational and IT-related goals. This goals cascade essentially offers a mechanism to translate stakeholder needs (e.g., benefits realization, risk optimization, and resource optimization) into specific, actionable, and customized organizational goals, IT-related goals, and enabler goals. This translation provides the ability to set specific goals at every level and area of an organization in support of the overall goals and stakeholder requirements. Although COBIT 5 allows organizations to set their own goals at every level, it offers a comprehensive set of goals for various levels that organizations can adopt as baseline outcomes and customize them as needed to fit with their unique requirements and contexts.

Building on the core principles shown in Figure 59.1, COBIT 5 prescribes a comprehensive set of 37 processes related to organizational IT activities that are under the purview of IT governance. Figure 59.2 illustrates these core processes of COBIT 5 that are divided into two broad categories: (a) governance of enterprise IT and (b) management of enterprise IT. As shown in Figure 59.2, the governance processes...
Processes for governance of enterprise IT
Evaluate, direct, and monitor (EDM)

- EDM01 Ensure governance framework setting and maintenance
- EDM02 Ensure benefits delivery
- EDM03 Ensure risk optimization
- EDM04 Ensure resource optimization
- EDM05 Ensure stakeholder transparency

Align, plan and organize (APO)

- AP001 Manage the IT management framework
- AP002 Manage strategy
- AP003 Manage enterprise architecture
- AP004 Manage innovation
- AP005 Manage portfolio
- AP006 Manage budget and costs
- AP007 Manage human resources
- AP008 Manage relationships
- AP009 Manage service agreements
- AP010 Manage suppliers
- AP011 Manage quality
- AP012 Manage risk
- AP013 Manage security

Build, acquire, and implement (BAI)

- BAI01 Manage programs and projects
- BAI02 Manage requirements definition
- BAI03 Manage solutions identification and build
- BAI04 Manage availability and capacity
- BAI05 Manage organizational change enablement
- BAI06 Manage changes
- BAI07 Manage change acceptance and transitioning
- BAI08 Manage knowledge
- BAI09 Manage assets
- BAI10 Manage configuration

Deliver, service, and support (DDS)

- DSS01 Manage operations
- DSS02 Manage service requests and incidents
- DSS03 Manage problems
- DSS04 Manage continuity
- DSS05 Manage security services
- DSS06 Manage business process controls

Monitor, evaluate, and assess (MEA)

- MEA01 Monitor, evaluate, and assess performance and conformance
- MEA02 Monitor, evaluate, and assess the system of internal control
- MEA03 Monitor, evaluate, and assess compliance with external requirements

FIGURE 59.2 COBIT 5 process reference model. (Adapted from http://www.isaca.org/COBIT/Documents/COBIT5-Laminate.pdf)
deal with the stakeholder governance objectives such as value delivery, risk optimization, and resource optimization, and include practices and activities aimed at evaluating strategic options, providing direction to IT, and monitoring the outcome. These activities are broadly categorized as Evaluate, Direct, and Monitor (EDM) processes or practices. Management processes deal with practices and activities that cover the responsibility areas related to PBRM (plan, build, run, and monitor) of enterprise IT. These processes are grouped into four broad categories: (a) Align, Plan, and Organize (APO), (b) Build, Acquire, and Implement (BAI), (c) Deliver, Service, and Support (DSS), and (d) Monitor, Evaluate, and Assess (MEA). COBIT 5 provides a comprehensive guideline related to each of these governance and management processes with respect to how it should be implemented (i.e., activities, inputs, and outputs), its goals and metrics, its relationship with IT-related goals, and key governance practices (who holds the decision rights and is held accountable for decision-making).

COBIT 5 is expected to offer a set of strategic and operational benefits to organizations that implement these processes (see Figure 59.2). These benefits include, but are not limited to: (a) maintaining high-quality information to support business decisions, (b) achieving strategic goals and realizing business benefits through the effective and innovative use of IT, (c) achieving operational excellence through reliable, efficient application of technology, (d) maintaining IT-related risk at an acceptable level, (e) optimizing the cost of IT services and technology, and (f) supporting compliance with relevant laws, regulations, contractual agreements, and policies (ISACA 2012). However, these intended benefits cannot be achieved if organizations fail to define and manage the enablers that help organizations achieve enterprise and IT-related goals. COBIT 5 provides guidelines related to how each of these enablers—that is: (a) principles, policies, and frameworks, (b) processes, (c) organizational structure, (d) culture, ethics, and behaviors, (e) information, (f) services, infrastructure, and applications, and (g) people, skills, and competencies—should be implemented, monitored, and measured to ensure effective implementation of COBIT and a high degree of alignment between IT and business.

59.2.2 IT Service Management Framework: ITIL

ITIL is considered the de facto industry framework for ITSM processes, practices, and delivery. ITIL has been around for more than 20 years. It was originally developed in the early 1980s by a government agency in the United Kingdom, Central Computer and Telecommunications Agency (CCTA), that later merged into the Office of Government Commerce (OGC), a division under the U.K. Treasury. The CCTA and later the OGC recognized the need for developing and implementing standardized processes for IT service delivery. As noted earlier, such standardization was needed because of the increasing complexity in the IT landscape characterized by obsolescence of mainframe-centric infrastructure, distributed computing, and geographically dispersed resources (Arraj 2010). Although such a landscape afforded organizations the potential for increasing flexibility and processing capabilities, it inevitably created a scope for inconsistent IT service delivery across the organization. In an attempt to reduce this inconsistency, organizations started looking for a framework that would help standardize IT service design and delivery.

ITIL was originally published as a collection of 31 associated books covering various aspects of ITSM practices and provisions. The principle of the ITIL framework was based on a process-based view of controlling and managing operations pioneered by W. Edwards Deming using a plan-do-check-act (PDCA) cycle. The early version of ITIL was adopted by many large organizations including government agencies in Europe in the 1990s. ITIL quickly became a cornerstone for ITSM by allowing organizations to take a disciplined approach to service support and delivery. As ITIL grew in popularity in Europe and beyond, and the IT landscape started to become complex, there was a need to revise the early version of ITIL to develop a more closely connected and consistent set of books. ITIL V2 was introduced in the 2000–2001 time period by consolidating the initial library of 31 books to a manageable set of seven books that were more accessible and affordable (Cartlidge et al. 2007; Whittleston 2012). ITIL V2 became the de facto standard for ITSM practices around the world. By the mid-2000s, it had been adopted and implemented
by thousands of organizations as a basis of effective ITSM practices (Cartlidge et al. 2007; Kneller 2010). In 2007, ITIL V3 was introduced by enhancing and consolidating ITIL V2. ITIL V3 consists of five core books covering the lifecycle of IT services. In addition to these five core books, there is a sixth book, the *Official Introduction* that offers an overview of the five books and an introduction to ITSM as a whole. The core books and the additional complementary publications by the U.K. OGC offer detailed guidance on the implementation of IT service lifecycle and associated processes, principles, practices, and methods (Cartlidge et al. 2007).

### 59.2.2.1 Overview of ITIL V3

As noted earlier, ITIL V3 adopted a lifecycle approach to IT services. Figure 59.3 illustrates the core stages of this lifecycle and associated processes. The lifecycle starts with the stage of *service strategy* in which IT and business strategists collaborate to develop IT service strategies that support and align with business strategy practices (Cartlidge et al. 2007; Kneller 2010). Some of the key processes related to service strategy are strategy generation, service portfolio management, and demand management. Once the IT service strategies are defined, an IT organization is in a position to enter the second stage, *service design*, in which the IT organization designs the overarching IT architecture and each IT service to meet business objectives practices (Cartlidge et al. 2007; Kneller 2010). Some key processes related to service design are service catalog management, service level management, capacity management, information security management, and IT service continuity management. The third stage,
service transition, helps an IT organization migrate its designed IT services into live environments. The key processes in this stage help an IT organization manage and control new services or changes in IT services. Some of these processes are change management, release and deployment management, transition planning and support, and service assets and configuration management. Once the transition is done, the fourth stage, service operation, helps an IT organization deliver and support operational IT services in such a way that they meet organizational needs and expectations (Cartlidge et al. 2007; Kneller 2010). The key processes related to service operation are event management, incident management, request fulfillment, problem management, and access management. Finally, the fifth stage, continual service improvement, helps an IT organization learn from experience and adopt an approach, which ensures continual evaluation and improvement of the quality of IT services and the overall maturity of ITSM service lifecycle and underlying processes (Cartlidge et al. 2007; Kneller 2010). The key processes related to continual service improvement are seven-step improvement process, service measurement, and service reporting.

The adoption and effective implementation of ITIL V3 are expected to offer several operational and strategic benefits to organizations. These benefits include, but are not limited to, alignment of IT services with organizational priorities and objectives; manageable IT costs; increased business productivity, efficiency, and effectiveness by making IT services more reliable and better; financial savings from improved resource management and reduced rework; effective change management; improved user and customer satisfaction with IT; and improved end-customer perception and brand image (Cartlidge et al. 2007; IT Governance Institute 2008a; Kneller 2010; Whittleston 2012). However, organizations may not be able to garner these benefits if they fail to implement ITIL effectively. We discuss challenges related to ITIL implementation later in this chapter.

59.2.3 Information Security Framework: ISO/IEC 27000 Series

Although the need for an information security framework and associated policies was felt by organizations in the 1980s and 1990s, it was not until 1995 when the first well-received best practice standard for ISM was published. Known as BS 7799, it was developed by the U.K. Government’s Department of Trade and Industry (DTI). BS 7799 had two parts—the first part, BS 7799-1, provided the best practices for ISM and the second part, BS 7799-2, provided specifications and guidance about using information security management systems (ISMS) to manage and control information security in an organization. BS 7799-1 was adopted by ISO as ISO/IEC 17799 in 2000 and was known as the Code of Practice for Information Security Management (Clinch 2009). ISO/IEC 17799 was later revised in 2005. Around this time, organizations across the world started placing significant importance on information security and IT risks because of the operational and strategic value of information and technologies as organizational assets. Recognizing the need for a broad set of standards to support a wide variety of information security-related issues, ISO chose to create a new numbering scheme to accommodate a whole family of information security standards. Consequently, the ISO/IEC 27000 family of information security standards was created and ISO 17799 was renamed ISO/IEC 27002 and BS 7799-2 became ISO/IEC 27001 (Clinch 2009).

ISO and IEC developed ISO/IEC 27000 as a family of information security standards to specify the fundamental principles, concepts, and vocabulary for the ISO/IEC 27000 series of documents. It is important to note that the scope of ISO/IEC 27000 framework is not limited to IT-related risks and security. These standards also provide best practices and guidelines to manage any aspects of information (e.g., data, documents, messages) that an organization and its members may produce and consume. The key concept of the ISO/IEC 27000 standard is the planning, development, implementation, and operation of a certifiable ISMS. According to these standards, an ISMS provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the protection of information assets to achieve business objectives based upon a risk assessment and the organization’s risk acceptance levels designed to effectively treat and manage risks (ISO/IEC 2009). Individual standards within the ISO/IEC 27000 family

© 2014 by Taylor & Francis Group, LLC
TABLE 59.2 ISO/IEC 27000 Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27000</td>
<td>Provides an overview of and/or introduction to the ISO/IEC 27000 standards as a whole and the specialist vocabulary used in this family of standards</td>
</tr>
<tr>
<td>ISO/IEC 27001</td>
<td>Provides the details of the Information Security Management System (ISMS) requirements standard; ISMS provides the underlying foundation for the ISO/IEC 27000 standards and is used as the baseline to certify organizations that are ISO/IEC 27000 compliant</td>
</tr>
<tr>
<td>ISO/IEC 27002</td>
<td>Provides the code of practice for information security management describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls</td>
</tr>
<tr>
<td>ISO/IEC 27003</td>
<td>Provides guidance on implementing ISO/IEC 27001 (i.e., ISMS)</td>
</tr>
<tr>
<td>ISO/IEC 27004</td>
<td>Provides guidance on information security management measurement</td>
</tr>
<tr>
<td>ISO/IEC 27005</td>
<td>Provides details of an information security risk management standard</td>
</tr>
<tr>
<td>ISO/IEC 27006</td>
<td>Provides a guide to the certification or registration process for accredited ISMS certification or registration bodies</td>
</tr>
<tr>
<td>ISO/IEC 27007</td>
<td>Provides a guide to auditing ISMS</td>
</tr>
<tr>
<td>ISO/IEC 27008</td>
<td>Provides guidelines for the auditing of technical security controls</td>
</tr>
<tr>
<td>ISO/IEC 27010</td>
<td>Provides guidance on information security management for intersector and interorganizational communications</td>
</tr>
<tr>
<td>ISO/IEC 27011</td>
<td>Provides a guideline for information security management for telecommunications organizations (also known as ITU X.1051)</td>
</tr>
<tr>
<td>ISO/IEC 27013</td>
<td>Provides guidance on the integrated/joint implementation of both ISO/IEC 20000–1 (derived from ITIL) and ISO/IEC 27001 (ISMS)</td>
</tr>
<tr>
<td>ISO/IEC 27014</td>
<td>Provides guidelines for the governance of information security</td>
</tr>
<tr>
<td>ISO/IEC 27015</td>
<td>Provides information security management guidelines for organizations in the financial services industry</td>
</tr>
<tr>
<td>ISO/IEC 27016</td>
<td>Provides guidelines for the economics of information security management</td>
</tr>
<tr>
<td>ISO/IEC 27017</td>
<td>Provides guidelines for the information security aspects of cloud computing</td>
</tr>
<tr>
<td>ISO/IEC 27018</td>
<td>Provides guidelines for the privacy aspects of cloud computing</td>
</tr>
<tr>
<td>ISO/IEC 27019</td>
<td>Provides guidelines related to information security for process control in the energy industry</td>
</tr>
<tr>
<td>ISO/IEC 27031</td>
<td>Provides an ICT (information and communication technology) focused standard on business continuity</td>
</tr>
<tr>
<td>ISO/IEC 27032</td>
<td>Provides guidelines for cybersecurity</td>
</tr>
<tr>
<td>ISO/IEC 27033</td>
<td>This standard will replace the multipart ISO/IEC 18028 standard on IT network security</td>
</tr>
<tr>
<td>ISO/IEC 27034</td>
<td>Provides guidelines on information security for IT applications</td>
</tr>
<tr>
<td>ISO/IEC 27035</td>
<td>Provides guidance on information security incident management</td>
</tr>
<tr>
<td>ISO/IEC 27036</td>
<td>Provides security guidelines for supplier relationships</td>
</tr>
<tr>
<td>ISO/IEC 27037</td>
<td>Provides guidelines for digital evidence</td>
</tr>
<tr>
<td>ISO/IEC 27038</td>
<td>Provides specifications for digital redaction</td>
</tr>
<tr>
<td>ISO/IEC 27039</td>
<td>Provides guidelines for concerns intrusion detection and prevention systems</td>
</tr>
<tr>
<td>ISO/IEC 27040</td>
<td>Provides guidelines on storage security</td>
</tr>
<tr>
<td>ISO/IEC 27041</td>
<td>Provides guidelines on assurance for digital evidence investigation methods</td>
</tr>
<tr>
<td>ISO/IEC 27042</td>
<td>Provides guidelines on analysis and interpretation of digital evidence</td>
</tr>
<tr>
<td>ISO/IEC 27043</td>
<td>Provides guidelines on digital evidence investigation principles and processes</td>
</tr>
<tr>
<td>ISO 27799</td>
<td>Provides health sector–specific ISMS implementation guidance based on ISO/IEC 27002</td>
</tr>
</tbody>
</table>


provide guidelines and best practices for planning, development, implementation, and operation of an ISMS and associated ISM components (e.g., IT network security or cybersecurity). Table 59.2 provides a list of ISO/IEC 27000 standards that are either published or under development.

### 59.2.3.1 Overview of ISO/IEC 27001 and 27002

Although individual standards within the ISO/IEC 27000 family provide valuable guidelines for managing and controlling different aspects of information security in an organization, there are two...
Information Technology Management Frameworks

standards—ISO/IEC 27001 and ISO/IEC 27002—that offer the key documents related to requirements and practices associated with ISMS. ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS, using a continual improvement approach (DiMaria 2012). This standard provides a detailed discussion of the following areas related to ISMS: general requirements, implementation process, management and operation, maintenance and improvement, documentation requirements, management responsibility, resource provision, training awareness, internal audits, management, and continual improvement (Clinch 2009). It also offers mapping with other standards, such as OECD (Organization for Economic Cooperation and Development) principles, ISO 9001 (i.e., a de facto quality management standard), and ISO 14001 (an environmental management standard) for organizations that have implemented these other standards (Clinch 2009; DiMaria 2012).

ISO/IEC 27001 is intended to be implemented and used along with ISO 27002, also known as Code of Practice for Information Security Management (DiMaria 2012). ISO/IEC 27002 offers guidance on interpretation and implementation of the list of specific security controls within ISO 27001 (DiMaria 2012). The standard provides a set of security controls in different areas of information security management and offers guidance on how organizations can achieve these control objectives. Figure 59.4 illustrates these security controls grouped into 15 core areas of information security management (e.g., risk management, asset management, access control, software development, incident management, business

![ISO/IEC 27002 control objectives](http://www.iso27001security.com/html/27002.html)

© 2014 by Taylor & Francis Group, LLC
59.2.4 Relationships among the IT Management Frameworks

It is important to note that although IT management frameworks were developed to meet different organizational needs with respect to managing IT assets and capabilities, these frameworks have noticeable overlaps and striking similarities. Indeed, these frameworks have processes and metrics that are conceptually similar. For instance, COBIT 5 has specific processes (and associated subprocesses, activities, inputs, outcomes, and metrics) related to managing service agreements (APO09), availability and capacity (BAI04), changes (BAI06), operations (DSS01), and service requests and incidents (DSS02) that are conceptually similar to some key processes of ITIL V3, such as service level management, availability management, capacity management, change management, event management, and incident management (see Figures 59.2 and 59.3). Similarly, both COBIT 5 and ITIL V3 have processes related to security management, the core focus of ISO/IEC 27000 standards. Although these conceptually similar processes have common goals, these processes are operationally different and offer differential levels of granularity with respect to subprocesses, activities, inputs, and outputs. For example, COBIT offers high-level processes and metrics that are relevant to an entire IT organization and provides a mechanism to align IT and organizational goals. While there are processes, metrics, and IT goals related to IT service and security in COBIT, these are typically not as comprehensive as they are in ITIL or in ISO/IEC 27000 because COBIT focuses on many other IT processes in addition to processes related to IT service and security (IT Governance Institute 2008a,b). Another key difference is that COBIT focuses on the maturity and control of high-level IT processes, whereas ITIL focuses on executional details of service-related processes. Unlike COBIT and ITIL, ISO/IEC 27000 frameworks do not offer detailed processes related to information security management. Instead, it offers a set of control objectives that organizations can incorporate in their security policy to protect their information assets (see Figure 59.4).

Although there are significant differences among IT management frameworks, it is important to note that these frameworks typically do not contradict each other and it is possible for them to peacefully coexist in an organizational setting. In fact, there have been significant efforts in the practitioners’ community regarding how these frameworks can be aligned and mapped with each other so that organizations can maximize implementation benefits (e.g., Clinch 2009; IT Governance Institute 2008a,b). These efforts have led into multiple publications by industry associations that provided comprehensive mapping of these frameworks with each other to help organizations implement an IT management framework without sacrificing the benefits they receive from other frameworks that they might have already implemented. For instance, the IT Governance Institute (2008b) offered a detailed mapping of how these frameworks complement each other’s different IT governance domains and provided guidelines on how organizations can align these frameworks for organizational benefits. Clinch (2009) offered a detailed overview of how ITIL and ISO/IEC 27000 standards are aligned with each other.

Consistent with the efforts in practitioner literature about the peaceful coexistence of IT management frameworks, we suggest that IT organizations are in a unique position to leverage the IT management frameworks for organizational benefits. Adoption, effective implementation, and mapping of these frameworks will help IT organizations manage and control IT as a routine part of organizational activities. As shown in Figure 59.5, an IT governance framework will help an organization establish a clear standard, consistent procedures, and unambiguous practices regarding the overall IT function of an organization that is aligned with organizational-level activities, goals, and strategies. Once an IT governance framework is established and in effect, other frameworks will be able to leverage its processes, metrics, and control objectives, and deliver additional values to specific areas—e.g., service management,
Information Technology Management Frameworks

security management, and project management, related to the IT functions of an organization. We view an IT governance framework as an underlying platform that enables an organization to embrace other more specific frameworks that provide much deeper consideration of different elements, such as policies, processes, measurements, and improvements related to specific areas of IT. Together these IT management frameworks will help organizations manage their IT functions effectively and efficiently, and ensure a high degree of IT-business alignment and convergence (King 2010).

59.3 Impacts of IT Management Frameworks

IT management frameworks have profound impacts on how organizations manage and control their IT functions. As noted earlier, these frameworks have gained widespread popularity in the late 1990s and early 2000s. During this time, organizations had started making significant investments in IT and sought ways to ensure positive returns from these investments. There was a need to develop and implement frameworks that could help organizations better manage IT functions, justify investments in IT, and garner benefits from IT. Although there has been limited scientific evidence regarding the impacts of IT management frameworks on organizational outcomes (with a few exceptions that we highlight in this section), the practitioner literature is replete with anecdotal evidence and cases about the positive impacts of IT management frameworks on organizations and its members. In this section, we discuss impacts of IT management frameworks on practice with a particular focus on the measurable benefits that organizations are able to gain from implementing these frameworks. We also discuss the current status of adoption and implementation of these standards and associated challenges.

59.3.1 IT Governance Framework: COBIT

59.3.1.1 Adoption and Implementation of COBIT

Given that COBIT 5 was released recently (2012), our discussion of COBIT adoption and implementation is primarily based on COBIT 4.1 and earlier releases. There are numerous organizations around the world that have implemented different aspects of COBIT and received significant benefits. We will provide a list of some major organizations that have implemented COBIT in the following section. It is important
to note that although COBIT offers a comprehensive set of goals, processes, metrics, actions, and implementation details, it allows organizations to fully customize these different components to meet unique organizational needs. COBIT does not enforce implementation of any of these components in any specific sequence. In order to help senior executives make effective decisions about components of COBIT, it offers different tools such as management guidelines and benchmarking tools using a maturity model framework. Further, ISACA and IT Governance Institute offer training programs for organizations that are interested in implementing COBIT. Overall, COBIT offers flexible implementation provisions allowing senior executives to select the specific goals, processes, and metrics that are applicable in their organizational context, determine the cost-benefit ratio of adopting these components, and implement the components that will be most beneficial to their organizations.

We note that implementation of COBIT is not an easy journey. It requires radical changes in senior executives’—both IT and non-IT—mindset regarding the value of IT in their organizations. Given that COBIT is a process-oriented framework that defines management and control of IT assets and decisions, it requires changes in existing processes in order to derive benefits from implementation. Further, COBIT implementation is a resource-intensive process because of changes in organizational processes, and the need for advisory services and extensive training during implementation. In addition to challenges related to change and resource management during implementation, there are other reasons for COBIT implementation failure. Ramanathan (2007) highlighted some of these reasons: (a) absence of a formal, documented strategy during implementation, (b) weak communication of strategy (i.e., there might be major communication gaps between IT and business, and the value of implementation may not be properly communicated to the stakeholders), (c) technology-driven projects (i.e., COBIT is essentially an organizational framework and should not be driven by technology), (d) lack of project ownership by business and senior executives, and (e) informal IT performance assessment (i.e., IT organization is not willing to embrace a formal performance assessment).

59.3.1.2 Impacts of COBIT on Practice

COBIT has been implemented by major organizations such as Oracle, MetLife, Blue Cross Blue Shield, ScotiaBank, National Stock Exchange of India, U.S. Department of Veterans Affairs, U.S. Department of Defense, European Parliament, Harley-Davidson, UNISYS Corporation, Fidelity Investments, Allstate, and Charles Schwab. These organizations have received numerous benefits from COBIT (ISACA 2012). For instance, Oracle was able to use COBIT matrices and mapping documents to make various IT frameworks fit together. It was also able to leverage the concepts in the COBIT-related materials to create discussion of health and maturity self-assessments, provide a line of sight between its activities and its business goals, bring predictability and reliability to how the IT group plans and manages the work across the enterprise, and complement its corporate planning cycle with an IT management cycle (ISACA 2012). Similarly, COBIT helped Unisys standardize its IT strategy to support global operations, align the IT infrastructure with the company’s overall business strategy, and help with Sarbanes-Oxley compliance (ISACA 2012). The U.S. Department of Veterans Affairs (VA), a government agency, was able to create a new organizational structure for centralized IT management based on COBIT that provided a framework for IT governance plans, structures, and investments at the VA (ISACA 2012). Recently, Rouyet and Spauwen (2011) suggested that COBIT can help align green business strategy with IT strategy. For example, they suggested that COBIT processes and metrics are flexible enough to align with business goals related to efficient energy use, public image aligned to environmental concerns, and environmental regulatory compliance.

59.3.2 IT Service Management Framework: ITIL

59.3.2.1 Adoption and Implementation of ITIL

There has been an increasing global trajectory of adoption and implementation of ITIL since 2004. Although ITIL was widely used in Europe in the 1990s and early 2000s, awareness and proliferation
related to ITIL within North American organizations started to accelerate between 2004 and 2006 (O’Donnell 2011). The adoption and implementation of ITIL are now considered mainstream; a majority of the Fortune 500 corporations have adopted and implemented some form of ITIL (O’Donnell 2011). A study conducted by the Forrester Group in 2011 revealed that about 24% of U.S. organizations have formally embarked on ITIL-based programs more than 5 years ago. These programs were less than 5 years old for the remaining 76% of organizations (Mann 2012). Although effective implementation of ITIL hinges on different technological, organizational, and environmental factors, industry reports have found that senior executives in the organization are the most influential drivers of successful ITIL programs, followed by the core ITSM team that manages the IT service lifecycle in the organization (O’Donnell 2011).

There are several challenges associated with ITIL implementation. Ho (2008) noted that resistance to ITIL is often rooted in fear, and suggested that the key to alleviating this resistance is education. As implementation of ITIL requires commitment to a multi-year project, it is often met with resistance by IT employees (directly) as well as non-IT employees (indirectly). Ho (2008) listed a set of ITIL fears, a major source of resistance to ITIL implementation, such as fear of change (i.e., unknown consequences of ITIL implementation), fear of measurement (i.e., a perceived loss of control), fear of perceived process rigidity (i.e., ITIL processes can be perceived to be inflexible), fear of cost (i.e., a large investment is required to implement ITIL), and fear of complexity (i.e., ITIL typically introduces new roles, processes, and complexity in organizations).

Even if an organization is able to overcome these fears through training and other interventions, there are possible implementation mistakes that can still prevent organizations from garnering benefits from ITIL implementation (Guglielmo 2008; Mann 2012; Kneller 2010). For example, organizations may design and develop IT services that do not fit with the organizational processes or do not meet organizational needs. In many cases, organizations fail to understand and take account of the ongoing operational cost that ITIL processes require. Many organizations take into consideration the one-off project cost for ITIL implementation and do not recognize the continual service-improvement stage of the IT service lifecycle. Consequently, these organizations fail to recognize the annual cost of ownership for each IT service (Kneller 2010). In many cases, organizations take a “shortcut” approach to implementing ITIL. These organizations fail to recognize that ITIL implementation requires a strategic vision, top management support, a strong business case, an effective communication strategy, and effective control mechanism (Guglielmo 2008; Kneller 2010). ITIL implementation will change the way IT delivers value to the rest of the organization and the way organizations manage IT. There is a need, therefore, to develop effective strategies and interventions to create a service culture and climate throughout the organization (Guglielmo 2008; Kneller 2010).

59.3.2.2 Impacts of ITIL on Practice

There is plenty of anecdotal evidence and numerous case studies that indicate positive impacts of ITIL implementation on organizations and employees. Major organizations from across the world, such as Microsoft, HP, Fujitsu, IBM, Target, Walmart, Staples, Citi, Bank of America, Barclay’s Bank, Sony, Disney, Boeing, Toyota, Bombardier, Eli Lilly, and Pfizer, have adopted and implemented ITIL and received significant benefits (Arraj 2010). In addition to these major organizations, there are literally thousands of other organizations of all industries and sizes that have embraced ITIL practices. A recent industry report revealed that ITIL implementation had significant positive impacts on various aspects of IT service delivery and IT employees who deliver IT services (O’Donnell 2011). A survey of 491 ITSM professionals found that ITIL improved quality of IT service (83% of respondents felt so), productivity (85% of respondents felt ITIL improved IT productivity), reputation with the business (65% of respondents felt ITIL was either beneficial or significantly beneficial to improving reputation with the business), and reduce operational cost (41% of respondents felt ITIL helped reduce operational costs by improving the quality of IT services). At the individual level, this report found that ITSM
professionals who are ITIL certified received better salaries than those in the average IT position. In fact, about 70% of ITSM professionals received an increase in their salary over the past year. In the academic literature, Gacenga et al. (2010) conducted a broad-based survey of ITIL implementation in three different countries—Australia, the United Kingdom, and the United States. The results indicated that while ITIL implementation had a positive influence at process-level outcomes, organizations failed to gain broad organizational-level benefits from ITIL because most organizations chose to implement only a subset of ITIL processes.

59.3.3 Information Security Framework: ISO/IEC 27000 Series

59.3.3.1 Adoption and Implementation of ISO/IEC 27000

ISO/IEC 27000 standards are still evolving with many individual standards that are still under development (see Table 59.2). While it is difficult to assess the adoption and implementation drivers and challenges related to these standards, a wide range of organizations have adopted ISO/IEC 27001 and ISO/IEC 27002. These organizations are from different industries and economic sectors, such as IT, software, manufacturing, construction, financial, staffing, shipping, pharmaceuticals, academia, telecom, lottery, security, consulting, insurance, health care, energy, and navigation (IsecT, Inc. 2012; DiMaria 2011). Many government agencies and international organizations, such as the United Nations, have adopted ISO/IEC 27001 for ISM. Given that organizations can receive certification if they comply with ISO/IEC 27001 standards, the number of certificates related to this standard is an acceptable measure of the current adoption level of this standard. There are over 7,200 ISO/IEC 27001 certified organizations in the world as of May 2011 (ISMS International User Group 2012). It is important to note that this total number has potentially been underestimated because reporting of certification status is completely voluntary and many organizations may never report their certification status. Further, ISO/IEC 27001 certificates are issued by multiple certification bodies, so there is no central database of organizations that have adopted these standards and are certified.

59.3.3.2 Impacts of ISO/IEC 27000 on Practice

Although we do not have accurate and complete data regarding the adoption of the ISO/IEC 27001 standard, we found that certifications have been increasing steadily at a rate of about 1000 per year (ISMS International User Group 2012). Again, reporting of certification is voluntary and it is thus possible the rate of increase is underestimated. Such an increasing trajectory of certifications suggests that many organizations that adopted this standard have received benefits from it. Nonetheless, there has been a dearth of academic and practitioner literature related to the impacts of ISO/IEC 27000 standards on organizations. We found a few cases that illustrated how ISO/IEC 27000 standards helped organizations achieve favorable organizational goals (British Standards Institution 2012). For instance, Cleardata, a document scanning and archiving company in the United Kingdom, needed to develop and implement an ISM framework to reassure its clients that it would manage their information and data security to the highest of standards. Cleardata needed to develop a structured framework to ensure that security objectives were met, compliance with laws and regulations was guaranteed, and new business and customer trust was gained. When they adopted ISO/IEC 27001 and got certified, Cleardata was able to win multiple contracts as a direct result of certification. In a different context, a government agency, the NHS Purchasing and Supply Agency of the Department of Health in the United Kingdom, was able to receive official recognition that its security measures were effective; it had a systematic framework for managing sensitive data, and was able to establish a formal standard for the operations of the IT organization. Following the adoption and certification of ISO/IEC 27001, the Agency never had a security incident caused by a staff member, was able to keep the network virus-free and hacker-free, and was able to encourage stakeholders to share information without any fear of security breach and data loss (British Standards Institution 2012).
59.4 Research Opportunities

We suggest that IT management frameworks provide many fruitful avenues for future research. These frameworks offer rich content with respect to principles, provisions, processes, and metrics that can be leveraged in research. Further, there are a multitude of outcomes (i.e., measures of performance indicators) and potential antecedents to these outcomes offered in these frameworks. These relationships also deliver many interesting and fruitful future research opportunities. Although there is a wide range of such opportunities, we provide a set of research directions that we believe will make significant impacts on both theory and practice related to IT management. In addition to leveraging the frameworks that we discuss in previous sections, we also review prior research in the areas of IT governance, ITSM, and information security to unearth scientific gaps in these research streams.

59.4.1 Review of IT Management Research

The literature on IT governance is rich and mature, and it has been around for almost 30 years. This popular stream of research has offered deep insights on issues related to how IT organizations and IT assets should be structured, managed, and controlled for organizational benefits. There have been several recent reviews of this stream that provide a comprehensive description of what we currently know in this literature (e.g., Guillemette and Pare 2012; Jewer and McKay 2012). These reviews have indicated that much prior research has focused on three broad areas: (a) design, development, and implementation of IT governance framework and/or decision-making structures that IT organizations can use to organize their activities (e.g., Kaarst-Brown 2005; Kaarst-Brown and Robey 1999); (b) antecedents and impacts of IT governance practices on organizational outcomes (e.g., Brown 1999; Sambamurthy and Zmud 1999; Weill and Ross 2004); and (c) the role and competencies of board and/or senior executives (both IT and business) in managing and controlling IT governance processes and activities (e.g., Leidner and Mackay 2007; Nolan and McFarlan 2005).

Notwithstanding the richness of research in these three broad areas, we suggest that the IT governance literature in general has overlooked issues related to various components of IT governance frameworks that are widely used in practice. IT governance frameworks such as COBIT offer rich descriptions of processes and their relationships with IT and organizational goals. Although prior research offered insights on governance structure and form, there has been limited research that incorporates various governance processes from COBIT, categorizes them into theoretically meaningful categories, and examines the impacts of these categories on various aspects of organizational outcomes. Such work will be beneficial to practitioners to justify the investments and efforts in IT governance processes and practices. Further, there has been limited research that focused on the measurement of IT governance effectiveness. Although IT governance frameworks such as COBIT offer a comprehensive set of performance indicators for various processes and practices, it is possible that many of these indicators are not scientifically valid and/or practically useful. Future research may organize these measures into theoretically meaningful categories and scientifically validate them for future research and practice.

Like the IT governance literature, the ITSM literature is mature and has offered insights on various aspects of ITSM practices in organizations. ITSM has been a focal topic in two distinct yet related streams of research. The first stream focuses on issues related to designing, developing, implementing, and managing IT services in organizations (e.g., Bardhan et al. 2010; Montoya et al. 2010). In this stream, researchers have concentrated on how organizations design, implement, and access IT services based on emerging IT services platform and architecture, such as application service providers (ASP), web services, service-oriented architecture (SOA), and cloud computing (e.g., Choi et al. 2010; Mueller et al. 2010; Susarla et al. 2003). This stream also deals with issues such as the impact of IT service sourcing and contracts (e.g., Benorach et al. 2010; Kauffman and Sougstad 2008).

Drawing on the service quality literature from marketing (Parasuraman et al. 1994; Zeithaml et al. 1996), the second stream deals with topics related to conceptualizing and measuring IT service
Managing Organizational Information Systems and Technology Capabilities

59-18

quality—in particular, the quality of IT functions in organizations (e.g., Kettinger and Lee 2005; Pitt et al. 1995). When IS researchers conceptualized and operationalized IT service quality, similar to the notion of service quality in the marketing literature (Parasuraman et al. 2005), they looked at people-delivered services. The key difference was that IS researchers focused not only on IT services (e.g., hardware and software installation) delivered by an entire IT department of an organization but also on the quality of service related to an individual IT system itself. In fact, Pitt et al. (1995) noted that there are two possible units of analysis for conceptualizing and measuring IS service quality (SERVQUAL)—the entire IT department and a particular IT application. While people-delivered services were the key focus initially in the IS literature, researchers have also examined technology-delivered services such as e-commerce websites (e.g., Parasuraman et al. 2005; Ziethaml et al. 2002).

Research on ITSM has either focused on IT infrastructure issues or the overall IT function of an organization while overlooking the specific ITSM processes that may offer differential value propositions for organizations. More importantly, prior ITSM research has focused primarily on IT-enabled service delivery. We are not aware of any research that highlights other stages of the ITSM life cycle, such as service strategy, service transition, and continual service improvement. These stages offer a set of processes, practices, and metrics that have been mostly overlooked in the extant literature. Further, there has been limited research that examined how ITSM processes and practices can lead to favorable outcomes for an IT organization in particular and the overall organization in general. Finally, prior research has offered a limited understanding of measuring the quality of ITSM practices. While SERVQUAL has provided a broad-based measure of ITSM quality, it is not an objective measure and does not capture the richness that an ITSM framework, such as ITIL, may offer.

The IT security literature gives rich insights on various aspects of ISM in organization, such as compliance, security behaviors, security policy decisions, and risk management. Research in this stream can be grouped into two broad categories. The first category is related to the behavioral issues of ISM such as individual compliance, security behaviors, and user involvement in ISM in organizations (e.g., Bulgurcu et al. 2010; Johnston and Warkentin 2010; Siponen and Vance 2010). This stream provides a comprehensive understanding of individual-level issues related to ISM processes and practices in organizations. For example, Bulgurcu et al. (2010) examined the factors that employees consider when they decide to comply with organizational security policies. The second category of IT security research is related to the development and implementation of organizational policies related to ISM and IT risk management (e.g., August and Tunca 2011; Chen et al. 2011). This stream of research employed both empirical and analytical approaches to unearth factors that have implications for organizational information security policies.

Although IT security research offers insights on both individual behaviors and organizational policies, we suggest that this research does not offer insights on the characteristics of a comprehensive ISMS, and antecedents and outcomes of establishing an ISMS. With the advances of technology and increasing complexity in the IT landscape, we suggest that ISM should be an important stream of IT research that focuses on both theoretical underpinnings related to ISM and practical considerations when implementing ISMS. Further, there has been little or no research that examined the value proposition of ISMS for organizations and scientifically validated the impacts of ISM practices on organizational outcomes.

59.4.2 Suggested Research Directions

Our goal is to offer a set of future research directions that address the gap in the current literature and leverage the richness that IT management frameworks offer. One of the rich components of each of these frameworks is performance measures—key performance indicators (KPIs)—for various aspects of IT management in organizations. For example, COBIT and ITIL frameworks and associated documents offer a comprehensive selection of measures to assess the performance of various processes and activities. These measures are now widely available and generally accepted among senior IT executives as indicators to measure performance of IT functions and services. While prior research has provided
various types of IT function assessment (e.g., Brown and Magill 1994; Chang and King 2005; Saunders and Jones 1992), we suggest that future research could leverage the rich performance indicators that IT management frameworks offer to measure performance of IT function in organizations. Thus, we offer the following opportunities for future research.

**Research Opportunity 1: Development of Performance Measures**

Development and validation of a new scale of (a) IT service quality measures using the ITIL framework; (b) effectiveness of IT governance practices and processes using the COBIT framework; and (c) effectiveness of ISM practices using the ISO/IEC 27001 and ISO/IEC 27002 standards. Is it possible to develop an overall performance scale for each of these areas, or should there be different scales for practices and processes within each of these areas?

In order to leverage the richness of IT management frameworks, it is important for researchers to dig deeper into the different processes and activities that these frameworks provide. These processes and activities indeed offer a detailed representation of what an IT organization does at strategic, tactical, and operational levels to manage IT functions in an organization and how it attempts to align with organizational activities and strategies. As noted earlier, there has been little or no research that has examined the impacts of these processes on outcomes related to IT and organizations. Given the comprehensive nature of these processes, it is probably not possible to incorporate the processes from an IT management framework in a single research inquiry. Therefore, we suggest that researchers try to categorize these processes into theoretical constructs and operationalize them following the guidelines from respective IT management frameworks. For example, researchers can develop three different categories of ITSM processes—strategic, tactical, and operational—and examine the impacts of these processes on outcomes related to IT and organizations. It is important to note that this categorization should be guided by a theoretical framework. We expect that researchers will be able to develop interesting theoretical constructs based on the IT management frameworks and offer theoretical insights on how these frameworks will influence IT and organizational outcomes. Based on this discussion, we propose the following research direction related to the impacts of different components of IT management frameworks.

**Research Opportunity 2: Impacts on Organizational Outcomes**

What are the impacts of IT governance/ITSM/ISM processes and activities on IT and organizational outcomes? What processes and activities have the most impacts and why? Is it possible to group these processes into theoretical constructs that will inform current organizational theories?

We suggest that IT management frameworks will have a proximal effect on IT outcomes and a distal effect on organizational outcomes. This distal effect could be mediated by the IT-related outcomes. We believe that these relationships have interesting theoretical implications that researchers should explore in future research. For example, it is important to understand what components of IT management frameworks will have a direct influence on organizational outcomes and what components will have a mediated influence through IT-related outcomes. Such an understanding will help IT organizations focus on certain components to achieve desired outcomes. Further, if researchers could show that certain IT outcomes need to be achieved first before garnering organizational benefits from an IT management framework implementation, IT organizations could focus on specific processes and activities to achieve those IT-related outcomes. Overall, we suggest that the dynamics of the relationship between different components of IT management framework and outcomes (both IT-related and organizational) is a fruitful avenue of future research that will have an immediate impact on practices related to IT management in organizations. Based on this discussion, we propose the following opportunity for future research.

**Research Opportunity 3: Impacts of Framework Components on Organizational Outcomes**

Do different components of IT management frameworks (e.g., processes and activities) have a direct impact on organizational outcomes such as productivity and profitability (as claimed in practitioner reports) or do they have a mediated impact through IT outcomes? How and why? What are the theoretical mechanisms that explain these relationships?
Gordon and Gordon (2002) discussed the tension between IT function and non-IT functions in organizations during IT service delivery. Both academic and practitioner literatures offer numerous examples of tension and the lack of trust between IT and non-IT functions in organizations. We suggest that IT management frameworks will offer new insights into the understanding of the relationship between IT and non-IT functions. These frameworks have specific processes, activities, and metrics related to how an IT organization should manage change and other IT assets that are exposed to end users and customers who are mostly dealing with non-IT functions. Further, these frameworks have specific goals and processes related to improving user and customer satisfaction. A fruitful area of future research will thus be to look into the issues related to the tension and the lack of trust between IT and non-IT functions and offer mechanisms (e.g., processes, practices, and activities) from IT management frameworks about how to resolve this tension and the lack of trust. Therefore, we offer the following research questions for future inquiries.

**Research Opportunity 4: Relationship between IT and Non-IT Functions/Users**

*What are the most effective components of IT management frameworks to improve user and customer satisfaction and trust between IT and non-IT functions? What are the components that may increase tension between IT and non-IT functions? What are the metrics to assess the relationship between IT and non-IT functions?*

We suggest that the effective implementation and practice of IT management frameworks will be a source of competitive advantage. While these frameworks are publicly available, we do not expect that all organizations will be able to equally implement and use them effectively. In fact, prior research has shown that publicly available best practices could be implemented and used differently by different organizations, leading to different outcomes (Bala and Venkatesh 2007; Venkatesh and Bala 2012). Based on this discussion, we suggest that organizations will be able to develop certain capabilities around IT management frameworks. For instance, some organizations will be able to develop capabilities related to effective IT governance (e.g., quick decision-making, formal performance evaluation, and high degree of knowledge sharing between IT and business), whereas other organizations may develop capabilities around ITSM practices. We expect that these capabilities will help organizations achieve favorable outcomes at both IT and organizational levels. Therefore, we offer the following research opportunity related to capabilities stemmed from implementing IT governance frameworks.

**Research Opportunity 5: Development of IT Management Capabilities**

*What are some of the capabilities organizations can develop around IT management frameworks? What are the dimensions of these capabilities? What provisions, processes, and activities will determine and define these capabilities?*

In sum, the research opportunities that we discuss here are broad and meant to serve as a guideline for researchers to develop more specific research questions for their research. We believe that these opportunities barely scratch the surface of the potential research space that IT management frameworks may offer. We expect that these opportunities will spur many fruitful research programs in the context of IT management frameworks.

### 59.5 Concluding Remarks

Our review of both practitioner and academic literatures indicates that although IT management frameworks, such as COBIT, ITIL, and ISO/IEC 27000, have been able to generate a wide range of interests and acceptance among senior executives who are interested in understanding how IT functions in an organization should be governed, managed, operated, and controlled, these frameworks have been conspicuously overlooked in mainstream academic research. While we acknowledge that academic research needs to be theory-driven (as opposed to framework-driven) and needs to offer theoretical insights about a phenomenon of interest, we suggest that IT researchers have a unique opportunity to conduct theory-driven research leveraging the richness of IT management frameworks. Recently, Mithas
et al. (2011) employed the Baldridge criteria, an industry framework to assess performance excellence developed by the National Institute of Standards and Technology (NIST), to conduct theory-driven research, and found strong support for the relationship between information management capability and firm performance. We suggest that IT researchers should undertake similar research in the context of IT management frameworks for at least two reasons.

First, we believe that such research will help the IT research community reduce the theory–practice (and the rigor-relevance) divide that is prominent in IT research. The details about this divide and associated debates have been outlined elsewhere (see for example, Benbasat and Zmud 1999; Constantinides et al. 2012; Davenport and Markus 1999). Recently, Rosemann and Vessey (2008) suggested that relevance for practice can be achieved by producing research that is important to practice, is accessible by practitioners, and can be assessed for relevance through applicability checks (Constantinides et al. 2012; see Rosemann and Vessey 2008 for details related to applicability check). Others have called for conducting high-visibility and high-impact research that has impacts on both theory and practice (e.g., Agarwal and Lucas 2005). In light of these views, we suggest that given the widespread acceptance of IT management frameworks, researchers may have a unique opportunity to help practitioners improve these frameworks and implement them effectively by offering insights from rigorous scientific research. We are not aware of any major scientific studies and associated publications that examined the implementation challenges, appropriate configuration, and impacts of these frameworks. Therefore, we suggest that such research will be able to help the IT research community reduce the gap between theory and practice in the context of IT management by helping practitioners improve the quality of these frameworks and the implementation process.

Second, we believe that the richness of IT management frameworks will help researchers develop valuable theoretical insights related to IT management practices in organizations. There has been much debate about the role of IT artifact in IT research. Scholars have called for placing an explicit emphasis on IT artifact in order to enhance the legitimacy of the discipline and to alleviate the identity crisis that the discipline currently faces (Benbasat and Zmud 2003; Constantinides et al. 2012; Orlikowski and Iacono 2001). We believe that research based on IT management frameworks will help researchers address this call by offering deep insights on how IT should be managed for organizational benefits. Further, prior research has called for incorporating the role of contexts in theory development (Johns 2006; Rousseau and Fried 2001). The components of IT management frameworks, such as processes, activities, inputs, outputs, and responsibility assignments, offer rich contexts to study various aspects of IT management practices in organizations. Researchers will be able to discover boundary conditions of existing organizational theories and offer novel theoretical perspectives leveraging the rich contexts that IT management frameworks may offer. For instance, using the resource-based view (RBV) of the firm theory, prior research has developed a comprehensive set of IT capabilities. While these capabilities are important, IT management frameworks can help researchers extend these capabilities by including other dimensions, such as IT service management capabilities, IT governance capabilities, and information security management capabilities. Overall, we suggest that IT management frameworks may offer opportunities for developing novel theoretical perspectives on IT management activities in organizations.

In conclusion, we reiterate our view that IT management frameworks are important for both theory and practice. We believe that these frameworks are here to stay and will improve over time to help organizations address the key concerns related to IT management (Luftman and Ben-Zvi 2011). Notwithstanding the implementation challenges we discuss in this chapter, there is an increasing trend of adoption and implementation of these frameworks. Therefore, we believe that it is high time to develop fruitful research programs around these frameworks. In this chapter we offer an overview of these frameworks and highlight that these frameworks can coexist peacefully in organizations. We also discuss the impacts of these frameworks on practices based on our extensive review of the practitioner literature. Our major contributions are the discussion of prior research and potential research opportunities based on these frameworks. Our hope is that this chapter will fuel future research and intellectual discourse on popular IT management frameworks.
Acknowledgments

We thank Professor Heikki Topi, Volume Editor, for his thoughtful comments and suggestions to improve the chapter. We thank Dr. Suzanne Van Hove, CEO of SED-IT, and Julie Montgomery, Director of Marketing of Plexent, for their support and encouragement for our project on IT management frameworks. We also thank Professor V. Sambamurthy (Michigan State University) for his guidance in helping us think about future research directions on IT management. Finally, we appreciate Akshay Bhagwatwar’s help in the literature review and background research on IT management frameworks.

References


© 2014 by Taylor & Francis Group, LLC


Information Technology Management Frameworks


