Fall 12-12-2010

Investigating the Relationship between IT and Organizations: A Research Trilogy

Benoit Raymond
Georgia State University

DISSERTATION

Investigating the Relationship between IT and Organizations: A Research Trilogy

Benoit Raymond
PhD Candidate - Computer Information Systems Department
J. Mack Robinson College of Business
Georgia State University
Atlanta, Georgia USA

COMMITTEE MEMBERS:

Chair:	Dr. Daniel Robey (GSU - Computer Information Systems)
Internal Examiners:	Dr. Richard L. Baskerville (GSU - Computer Information Systems)
	Dr. Balasubramaniam Ramesh (GSU - Computer Information Systems)
External Examiner:	Dr. Ram S. Sriram (GSU - School of Accountancy)

Final Oral Examination: December 3, 2010

Table of Contents

Introduction

The overall research objective of this dissertation is to contribute to knowledge and theory about the influence of information technology (IT) on organizations and their members. This dissertation is based on a multi-paper format and, as such, is composed of three complete and related studies. While the three studies are complementary, each study has its own research objective, adopts a unique research perspective and examines different aspects of the relationship between IT and organizations. The next section describes the motivation and research objective of each study as well as its links with the overall theme and the other studies included in this dissertation. The order of presentation of the three studies composing this dissertation is based on the breadth of their scope, starting with the most general study and ending with the most specific study.

First Study: The Relationship between IT and Organizations: Review of Theoretical Perspectives over Half a Century

Motivation and Research Objective

Since its implementation in organizations, IT has been associated with organizational change, being often considered as a condition or occasion for it. Practitioners and researchers have been intrigued by the influence of IT on organizations and their members.

The objective of this study is to provide an overview of the dominant theoretical perspectives that IS researchers have used in the last five decades to study the influence of technology on organizations and their members. Without being exhaustive, this study seeks more specifically to

identify, for each decade, the dominant theoretical perspectives used in the IS field. Moreover, these dominant theoretical perspectives will be illustrated by the selection and description of exemplars published in the decade and their implications for researchers and practitioners will be discussed. This review is useful not only for understanding past trends and the current state of research in this area but also to foresee its future directions and guide researchers in their future research on the influence of IT on organizations and their members.

Links with the overall research objective and the other studies in this dissertation

Looking at the theoretical perspectives that IS researchers have used in the last five decades to study the relationship between IT and organizations, this study is directly related to the overall theme of this dissertation. Furthermore, because it provides a fifty-year overview of theoretical perspectives used in this research area, this study has the broadest scope and serves as a general frame and introduction for the two other and more specific studies of this dissertation.

Second Study: How IT Artifacts Influence the Design and Performance of Organizational Routines: Extending Organizational Routines Theory

Motivation and Research Objective

For many years, research on IS post-adoption behavior has favored human agency as the main determinant for most of what happens after information systems are implemented and initially adopted. By putting a large emphasis on human agency, voluntarist theory treats IT as almost indefinitely malleable and interpretively flexible and, as such, somewhat neglects the role of materiality of artifacts.

Aiming at providing new insights about IS post-adoption behavior, this study adopts a different research perspective in which material aspects of technology play a more central role as they can both enable and constrain human action without determining it. More specifically, the objective of this study is to theorize how IT artifacts influence the design and performance of organizational routines. This research objective is motivated by the fact that organizational routines represent an important part of almost every organization as work is usually organized and accomplished via organizational rules and work processes involving multiple participants. Moreover, compared to individual routines and interactions with a technology, organizational routines involve multiple actors and interdependent actions which further constrain individual agency. This study adopts organizational routines theory as its theoretical lens. Organizational routines theory is an influential theory that explains how the accomplishment of organizational routines can contribute to both organizational stability and change. However, the current form of this theory has several limitations such as its neglect of the material aspect of artifacts and the distinctive characteristics of IT artifacts, and its treatment of artifacts as outside of organizational routines. This study seeks to overcome these limitations by extending organizational routines theory.

Links with the overall research objective and the other studies of this dissertation

Because organizational routines are at the core of organizations, the study of the influence of IT artifacts on the design and performance of organizational routines represents an effective way to investigate the relationship between IT and organizations.

This study can be related to the other papers included in my dissertation. The first study can be seen as providing an overview of theoretical perspectives and research about the influence of IT on the accomplishment of organizational routines over the last fifty years. This study explains that IT has not only automated many of manual work processes in organizational routines, making them more effective and efficient, but also caused important changes to various aspects of organizational routines, such as changes to roles and task definitions. The third study can be seen as presenting the specific case of how information security risks associated with the use of IT in organizations influence the design and performance of organizational routines.

Third Study: Generative Control Theory for Information Systems

Motivation and Research Objective

Increasing information security losses, coupled with more closely regulated security risk disclosure, are raising the importance of information security standards in designing information security. Despite the growing importance and number of these standards and the fact that their adoption requires a large investment, there is a lack of theoretical development in this area. The objective of this study is to develop a better understanding of information security standards by analyzing the structure and content of their controls. More specifically, this study is interested in understanding how various information security standards may differ in the nature, structure and coverage of their controls depending on their goals. Moreover, it investigates the mechanisms used in the design of information security standards to made them applicable to a wide range of organizations while, at the same time, enabling their own adaptation to various specific

organizational settings. The results of this study led to the proposition of a new theory for information systems called generative control theory.

Links with the overall research objective and the other papers of this dissertation

Information security is an important aspect of the relationship between IT and organizations. The implementation and use of IT in organizations increase information security risks which, in turn, motivate the application of information security controls and the development of information security standards. These information security controls and standards, in turn, affect the design of the IT infrastructure and the use and management of IT in organizations.

This study can be related to the first study of my dissertation. The first study can be seen as providing an fifty-year overview of how the implementation of IT in organizations over time influenced the way organizational information is processed, stored, accessed, communicated and managed. As mentioned earlier, this has an impact on information security risks and the development of information security controls and standards to mitigate them.

This study can also be considered as the application of concepts presented in the second paper of this dissertation to the study of information security standards. Information security standards and their controls may be considered as IT artifacts embedded in organizational routines, thus representing an integral part of these routines. According to generative control theory, an important part of information security standards is comprised of generative controls that defer the specific design and implementation of more precise information security controls to people inside the adopting organizations. As generative controls' broad definition serves to generate

more precise controls, they can be related to the ostensive aspect (abstract idea) of the organizational routine. In turn, the more precise controls that are generated from generative controls can be related to the performative aspect (varying performances) of the organizational routine. Because the broad definition of generative controls can be interpreted in different ways, the specific design and implementation of precise controls are likely to be different across adopting organizations. This introduces variations, or new performances, regarding the implementation of the standard. As such, the role of standard compliance auditors represents the legitimating process for novel standard's implementations (performances) as auditors need to assess if these variations increase or not information security risks for the adopting organization.

Additional Contributions of this Dissertation

In addition to the research objectives of the three studies composing this dissertation, this dissertation aims at providing novel insights on various aspects related to the relationship between IT and organizations. For instance, an important aspect relates to IT post-adoption behavior which has strong practical and theoretical implications. The decision to implement a new IT can be seen as a risky project, usually involving a lot of resources (time, human and financial) but producing unpredictable outcomes as many IT post-adoption issues can arise. Interestingly, the initial acceptance of technology by end users does not seem to guarantee that the technology will continue to be used, and thus generate its benefits long after its implementation. In its study of professional virtual communities, Chen (2007) found that initial use (acceptance) is merely the first step toward realizing organizational success as such success will further depend on members' continued use (or usage continuance) of the technology. In their study of EDI implementation, Morris et al. (2003) found that short-term usage of EDIs was

unlikely to result in significant organizational change, but long-term usage was. Therefore, it is possible that a project that initially resulted in the successful implementation and adoption of a technology later transforms itself into a failure. This is why researchers need to better understand the factors and dynamics involved in IT post-adoption behavior. Managers need to be able to identify and manage IT post-adoption issues in a timely and appropriate manner.

Another important aspect relates to the use of information system (IS) packages as they represent a different kind of software. Indeed, compared to custom-made ISs, IS packages offer many differences in terms of design, functionality, and work processes. Because IS packages incorporate standard work processes, they can be seen as more rigid and constraining than custom-made ISs for organizations implementing them. These differences between IS packages and custom-made ISs are likely to have an impact on how these ITs influence organizations. Kallinikos (2004), reflecting on the comprehensive character of IS packages and the issues their diffusion raises, suggested that they presumably mark a distinctive stage in the history of computer-based information technology's involvement in organizations. Therefore, it seems important for both practitioners and researchers to understand how the distinctive and material characteristics of IS packages affect the influence of the IT artifact on organizations and their members.

Finally, this dissertation provides insights about the theoretical aspects of the relationship between IT and organizations. Technology can be considered as both constraining, thus acting as a constraint, and enabling human action, thus contributing to the expression of human agency. The theoretical treatment of technology, and more generally artifacts, is an important issue

generating several debates. For instance, should technology be treated as an integral part of organizational work processes or outside them, as part of their environment? Can technology be considered as a structure? Can structures be embedded in a technology? These theoretical issues have important implications for understanding how IT can influence organizational work processes and organizations in general.

The Relationship between IT and Organizations: Review of Theoretical Perspectives over Half a Century

Benoit Raymond
Computer Information Systems Department
J. Mack Robinson College of Business
Georgia State University
Atlanta, Georgia USA

Abstract

This study provides an overview of the dominant theoretical perspectives that IS researchers have used to study the influence of technology on organizations and their members in the last five decades. Without being exhaustive, our review of IS literature identifies, for each decade, the dominant theoretical perspectives used in the IS field. We illustrate them by selecting and describing two exemplars published in the decade and explain their implications for researchers and practitioners. The results of this study show that in each of the last five decades, a new dominant theoretical perspective was developed and adopted to extend the previous decade's rhetoric by getting even further away from technological determinism in the sixties and closer to more balanced causal arguments explaining the consequences of IT on organizations and their members. Our analysis suggests important implications for future research such as the need for IS researchers to study and theorize the materiality of IT artifacts and potential approaches that IS researchers can use by for restoring theoretical attention to material IT artifacts in IS research.

Introduction

Since the fifties a persistent rhetoric is that information technology (IT) is typically assumed to be associated with organizational change. IT has important implications for organizational design, being often considered as a condition or occasion for change in numerous aspects of organizations and their members such as organizational roles, structures and processes. The tremendous and accelerating advances in IT since this time period have not decreased practitioners' and researchers' interest in how IT is contributing to organizational change. Over these years, information system (IS) researchers have adopted a variety of theoretical perspectives to understand this phenomenon and offered a progression of explanations to explain it.

The objective of this study is to provide a broad historic overview of the dominant theoretical perspectives that IS researchers have used to study the influence of technology on organizations and their members over the last five decades. In this study, we use the term IT, which has a broad meaning, to refer to a large range of technologies such as communication and collaborative technologies, personal computers, and functional and enterprise information systems. Motivating this study is our hypothesis that there have been important shifts in IS theoretical perspectives over this time period. While certainly not exhaustive, this review of the dominant theoretical perspectives used by IS researchers is important for several reasons.

Identifying and understanding shifts in the dominant IS theoretical perspectives over the last fifty years is important to understand past trends and the current state of IT research in this area. These shifts reflect changes not only in rhetorics surrounding IT and organizations but also in the

importance of aspects of the reality of using IT in organizations. Moreover, this review highlights the different ontological and epistemological positions adopted by IS researchers over time as well as their specific issues and contrasts between them. Finally, this study provides insights into the emergence of new theoretical perspectives and how IS researchers can benefit from their adoption when they investigate the influence of IT on organizations and their members.

This paper is structured as follows. First, we describe the research method used for this study. Second, we present the results of this study, classified by separate time periods representing the last five decades. Third, we analyze and discuss the results of this study and provide directions for future research in this area.

Research Method

Search Parameters

For this paper, we decided to limit the scope of our literature review by reviewing only publications looking at the influence of technology on organizations and their members and published between 1960 and 2010 inclusively. As such, we specifically excluded research focusing on individuals and on society. This study was conducted using a combination of two research methods. First, a formal search of publications has been performed, based on a set of keywords related to the influence of IT on organizations and their members and using EBSCO as the search engine. More specifically, the literature search was based on the following keywords:

Use	Evaluate	Satisfaction
Understand	Implication	Benefit
Value	Impact	Participation
Practice	Routinized	Enacted
Transformation		

For each keyword, common alternative spellings and wording were included for double check. For example, to identify "IT", we have used synonyms like "information technology", "information system", and "system". To identify "influence", we have used partly synonymous concepts such as "impact", "implication". To identify "organizational structure", we have also surveyed the words "company", "job", and "role". We performed the keywords search one keyword and one journal at a time for all years surveyed. More specifically, the literature search covered publications from the following journals and year spans:

- MIS Quarterly (Impact Factor: 5.826): 1984-2008
- Journal of Management Information Systems (Impact Factor: 1.867): 1999-2008
- Information & Management (Impact Factor: 1.631); 1983-2008

These journals represent high quality journals that have been around for many years. Second, since many early IS studies are not readily available in electronic format and relevant publications may have escaped our keyword-based search, an informal attempt has been made in a second step, to identify seminal IS studies and important theoretical perspectives. This has been done following a "tracer approach", in which newer publications have been used to trace their sources, and then these sources were used to trace the own references.

Data Analysis

The list of publications obtained from the two research methods was then screened for their relevance to the main focus of this study: IT influence on organizations and their members. Publications judged irrelevant were discarded. Relevant publications were then classified in the last five decades covered by this study based on their publication date. Despite the fact that the normal time to market or delay between the submission and publication of research is about two years, we decided to use the publication dates as the reference for time in our classification of studies. This should be taken into account when interpreting the data.

Selection of Exemplars

Finally, the publications were analyzed in order to select, for each decade, at least two studies that are highly representative of the dominant rhetoric of that specific time period. These studies serve as exemplars of the dominant rhetoric in that specific period and are discussed to show how this dominant rhetoric is expressed and reflected in the findings and contributions of each study. The next section presents the results of this study, classified by decade.

Results

1960s

1. Summary of Dominant Rhetoric for this Period

The dominant rhetoric for this decade can be referred to as *technological determinism***.** As one of the earliest IS research perspective, it adopts a deterministic stance by considering technology (or a specific set of technological features) as an external force, independent of human action, producing significant, inevitable and predictable impacts on organizations and their members

(Leonardi and Barley 2008; Markus and Robey 1988; Orlikowski 2010). In this research perspective, technology (or artifacts in general) is seen as an independent variable that would shape organizational life by determining or strongly constraining the behavior of individuals and organizations (Markus and Robey 1988) and through impacts assumed to be fixed and final once the technology is implemented and adopted in organizations (Dutta 2008). Indeed, human agents are perceived to be powerless in presence of technology and social outcomes are assumed to emanate from the characteristics of a technology, regardless of users intentions (Markus 2005). This technological determinism perspective is consistent with Pfeffer's (1982) situational control perspective in which human action is seen not as the result of conscious, foresightful choice but as the result of external factors, events, constraints, demands, or forces that constrain or force people and organizations to behave in certain ways for which the social actor may have little control over or even cognizance of.

2. Exemplars

Exemplar 1: Burlingame (1961)

In his study, Burlingame (1961) challenged the deterministic predictions that computers and associated technologies will lead to the elimination of middle managers and the reversal of the trend of the last decade toward decentralization in business. Instead, Burlingame (1961) argues that decentralization and the middle manager are much more likely to grow in importance in the future with the use of computers in organizations.

Exemplar 2: Whisler (1965)

Whisler (1965) looked at deterministic predictions made about the effect of information technology on the manager and his organization structure. He found evidence supporting the deterministic prediction that IT will make the organization structure flatter by eliminating middle management levels or reducing the number of managerial positions. However, Whisler (1965) noted that this flattening of the organization structure was not due to the removal of a whole layer of management as predicted. Instead, Whisler (1965) found that it was due to the redistribution of tasks and responsibilities between organizational roles as the computer took over some parts of various positions.

Moreover, Whisler (1965) rejects the deterministic prediction that IT routinizes many of the middle management positions in the reorganized structure. He explains that the IT advantage lies in the computation part of the manager's job. Since much of the manager's job is to communicate with different people, Whisler (1965) argues that delegating the computation part to IT will only make the communication part of the manager's job proportionately more important.

Whisler (1965) also found evidence supporting the deterministic prediction that IT recentralizes control, and thus power, in organizations. However, he argues that this recentralization of control is only an interim impact of IT. Whisler (1965) predicts that as the functions of the manager and of IT become increasingly differentiated, the creative managerial functions retained by managers will be decentralized while the operating functions executed by IT will be centralized.

Interestingly, Whisler (1965) also established its own set of deterministic predictions about the consequences of IT on organizations. For instance, he predicted that managers will be displaced and will need retraining and that organization structures must be disassembled and rearranged into new forms. Moreover, he predicted that all members of the organization will need to adapt to a new technique and rhythm of planning as IT permits short-range planning to be done much more frequently with greater accuracy and long-range strategic planning to be extended further into the future through the use of appropriate simulation techniques. As such, Whisler (1965) explains that managers will become more the question-askers and computers, the question-answerers. Finally, Whisler (1965) predicted that the growth of required managerial knowledge will lead to the replacement of the traditional hierarchy with a single chief with the use of multiple chiefs or a committee top management.

3. Implications for Researchers and Practitioners

Early research on the relationship between technology and organizations was mainly composed of studies about production or manufacturing technologies. The fact that these technologies were seen as mostly fixed, rigid, and not readily adaptable by end users may have contributed to the adoption of a technological determinism research perspective. Although, IT may be seen as having distinctive characteristics and being more adaptable and thus less deterministic, IT was treated in the same way as production technologies, thus treated deterministically. Adopting this research perspective meant that organizational design was a matter of matching the right organizational structure to the technology used in the organization while moderating the predictable and inevitable impacts of technology on organizations was a matter of stopping,

slowing or accelerating the rate of change in technology or selecting technology with specific sets of features (Markus and Robey 1988).

However, researchers and practitioners should be aware that, as demonstrated in the two examplars, many of the deterministic predictions made about the consequences of IT on organizations and their members were not supported by empirical evidence. Morever, even the deterministic predictions that were empirically supported were often supported by other factors or arguments than the ones initially stated by their authors. While the technological determinism perspective has a long history and makes some compelling claims, empirical research has generated contradictory findings on almost every dimension of hypothesized computer impact (Markus and Robey 1988; Robey 1977). Markus and Robey (1988) explain that information systems have been found both to enrich and routinize jobs, both centralize and decentralize authority (Dawson and McLaughlin 1986; Klatzky 1970), and produce unexpected effects (Boudreau and Robey 2005).

1970s

1. Summary of Dominant Rhetoric for this Period

IS research in the seventies continued to be dominated by the deterministic assumption that technology will produce predictable and inevitable impacts on organizations and their members. However, the discovery of an increasing number of contradictory findings motivated researchers to investigate the existence of conditions or contingencies explaining these unexpected results and why different managerial approaches could produce the same results. These researchers adopted a more nuanced approach to technological determinism called the *contingency*

perspective that eventually led to the development of contingency theory. The contingency perspective continues to consider technology as an independent variable but it recognizes that the impact of technology is contingent on the fit with other independent variables (Markus and Robey 1988) As such, contingency theory stipulates that effectiveness results from the fit between organizational structure and contingencies. Examples of contingencies are technology, organizational size and level, decision making style, and environmental uncertainty (Markus and Robey 1988). Interestingly, while deterministic accounts of technological impacts were softened by the acknowledgement of various contingencies, a strong commitment to the conception of technology as a material and causal determinant of human action and organizational aspects, independent of humans and organizations, has continued to inform the deterministic research perspective (Orlikowski 2010).

The interest in contingencies to explain IT impacts on organizations and their members also led to the adoption of another research perspective called the *organizational imperative* perspective. This perspective assumes that people act purposefully to accomplish intended objectives, viewing the motives and actions of human actors as a cause of organizational change (Markus and Robey 1988). They explains that in the organizational imperative perspective, IT is seen as a tool for solving organizational problems, acting as the dependent variable caused by the organization's information processing needs and manager's choice about how to satisfy them. The organizational imperative perspective assumes that human actors can design and use information systems in almost unlimited ways to satisfy organizational needs and manage their impacts with almost unlimited control by attending to both technical and social concerns (Markus and Robey 1988).

The organizational imperative perspective is consistent with Pfeffer's (1982) "*intendedly rational*" perspective on action. According to Pfeffer (1982), this perspective assumes that human action is goal directed and resulting from prior free rational choices based on the evaluation of alternative courses of action or a set of consistent preferences. Moreover, this decade has also seen the development of other research perspectives. The so-called *socio-technical* perspective was spearheaded by Mumford (e.g. in the Ethics method), and the *political* perspective.

2. Exemplars

Exemplar 1: Jay Galbraith (1974)

Jay Galbraith is arguably the organization design author most representative of the contingency approach to IT in this decade. According to Galbraith (1974), the greater the task uncertainty (a contingency), the greater the amount of information that must be processed among decision makers during task execution to achieve a given level of performance. Adopting an organizational imperative perspective, Galbraith (1974) developed a framework integrating the various organization design strategies available to organizations to meet the increased information processing needs generated by task uncertainty. The framework suggests organizational interventions for either increasing the organization's capacity to process information or reducing its need for information processing. For example, Galbraith (1974) proposes that managers may reduce the need to process information by using rules or programs to coordinate behavior between interdependent routine predictable tasks. He also suggests that

managers can increase their organization's capacity to process information by investing in vertical information systems.

Exemplar 2: Robey (1977)

Robey (1977) got interested in the fact that many studies conducted during the 1960s and early 1970s showed conflicting findings regarding the effects of computer adoption on centralization and decentralization. In order to better understand these contradictory forecasts, Robey (1977) reviewed the cases, mostly case studies of conversions from manual work to computer-based work, by looking more specifically to their descriptions of environmental factors (e.g., competition, regulation). As such, he was looking for contingencies affecting IT impacts on organizations and their members. Robey (1977) observed that (1) computers do not cause changes in the degree of decentralization, (2) computerized systems are sufficiently flexible to facilitate either centralized or decentralized structures, and (3) the degree of decentralization in these studies is related to task environmental conditions of the organizations studied. He found that IT appeared to support an existing decentralized structure in organizations with uncertain environments. However, in simple environments, IT appeared to strengthen a centralized authority structure. Robey (1977) proposed to view IT as a moderating variable, affecting the strength of a causal relationship between environmental uncertainty and organizational structure.

3. Implications for Researchers and Practitioners

According to the organizational imperative perspective, the impacts of IT can be attributed to the choices and behaviors of managers and system designers (Markus and Robey 1988) as this perspective assumes the supremacy of human agency in the design and use of information

systems and the management of their impacts on organizations and their members. Contextual variables that might be viewed as constraints or determinants in a technological determinism or situational control perspectives are seen as contingencies that managers should take into account in the organizational imperative perspective (Markus and Robey 1988). As a result, they explain that researchers adopting this perspective prescribe the use of better design, resource allocation methods and implementation strategies and tactics to achieve expected results. Adopting an organizational imperative perspective, Galbraith's (1974) study provides a good example of how managers can use IT as a tool in organizational interventions to solve the organization's information processing needs. However, it is worth noting that empirical support for the organizational imperative is limited (Markus and Robey 1988).

According to the contingency perspective, the impact of technology can be seen as contingent on the fit with other independent variables. As such, researchers and managers must recognize the importance of not only technology but also the specific context or environment of the task or organization. For instance, Robey (1977) found that the degree of decentralization was caused not by IT itself but by task environmental uncertainty. Instead, he found that IT was moderating the strength of the causal relationship between environmental uncertainty and organizational structure. Noting that IT was associated with decentralization in uncertain environments, and centralization in certain environments, Robey (1977) proposed to view IT as a sufficiently flexible tool to facilitate either centralized or decentralized structures, thus softening deterministic predictions about the impacts of IT.

1980s

1. Summary of Dominant Rhetoric for this Period

In the eighties, researchers such as Markus & Robey (1988) started to challenge the still dominant technological determinism research perspective by trying to explain the contradictory outcomes of IT. They proposed the adoption of an *emergent process* perspective arguing that uses and consequences of technology emerge from the ongoing, complex and unpredictable interaction of people, technology and context. This perspective views technologies as socially defined and produced, grounded in specific historical and cultural contexts and dependent on specific meanings and contingent processes (Orlikowski 2010). She explains that understandings of technology are neither fixed nor universal, but emerge from situated and reciprocal processes of interpreting and interacting with particular artifacts over time. Compared to the deterministic causal arguments of the previous two decades, the emergent process perspective does not acknowledge a dominant cause of change (Markus and Robey 1988). As such, they explain that a detailed understanding of the dynamic organizational processes and knowledge about the intentions of actors and the features of IT are required to make predictions about the consequences of IT.

This emergent process perspective is consistent with Pfeffer's (1982) "emergent" perspective on action in organizations, in which the behavior of people and organizations emerges from a dynamic interaction of external circumstances and internal motives or interests. "Because participation in organizational decisions is both segmented and discontinuous, because preferences develop and change over time, and because the interpretation of the results of actions—the meaning of history—is often problematic; behavior cannot be predicted a priori

either by the intentions of individual actors or by the conditions of the environment" (Pfeffer 1982, p. 9).

2. Exemplars

Exemplar 1: Dawson and McLoughlin (1986)

Dawson and McLoughlin (1986) examined the implications for supervision of British Rail's attempt to computerize the control of its freight operations. More specifically, their objective was to find whether IT, by providing up-to-date accurate information about local operations to management, erode the importance of supervision in relation to management control as predicted in the literature. Dawson and McLoughlin (1986) found that the availability of up-to-date accurate information about local operations provided by IT enabled a centralization of overall control at regional and national headquarters while it also enhanced the role played by local supervisors by making possible to delegate responsibility for day-to-day decisions from divisional level. They explain that although the basis of the supervisor's autonomy within the marshalling yard prior to computerization was eroded, the overall effect was to integrate supervision into the management control system by creating a new supervisory role responsible for area freight operations.

Exemplar 2: Millman and Hartwick (1987)

Surveying 75 middle managers about their perceptions of the impact of automated office systems on their job and work, Millman and Hartwick (1987) found that middle managers perceived that office automation has led to a variety of changes that, almost without exception, made their jobs and work more enriching and satisfying. Moreover, they found that middle managers with first-

hand experience with various systems were even more positive than managers without this exposure. Millman and Hartwick (1987) explain that multiple processes are apt to be present during the introduction and use of various automated office systems. For instance, the process of using IT artifacts may lead to the development of perceptions about them. It is also possible that the development of perceptions about an IT artifact lead to its actual use. The presence of these multiple and concurrent processes occurring during the introduction and use of various automated office systems is likely to have a variety of direct effects, due to greater efficiency and effectiveness of the systems themselves, and indirect effects, due to the greater enrichment and satisfaction of jobs and work on middle managers and their jobs and work (Millman and Hartwick 1987).

3. Implications for Researchers and Practitioners

The emergent process perspective helps to explain the conflicting research findings about the impacts of IT on organizations and their members by highlighting the indeterminate nature of the consequences resulting from the use of IT. Indeed, an emergent process perspective assumes that uses and consequences of technology emerge from the ongoing, complex and unpredictable interaction of people, technology and context (Markus & Robey 1988) and that the same technology can acquire different meanings in different social settings (Orlikowski 2010). As a result, some researchers adopting an emergent process perspective may eschew intervention, arguing that prediction is impossible and outcomes are indeterminate (Markus & Robey 1988) while others may advocate "emancipatory" strategies, such as extensive user participation in the analysis, design, and implementation of information technology to minimize negative consequences of this emergent process (Markus & Robey 1988).

Dawson and McLoughlin (1986) observed that IT can both enable the decentralization of decisions to supervisory roles and increase management control over local operations. As such, they demonstrated that the introduction and use of IT in an organization is better seen as an emergent process with indeterminate outcomes rather than a simple management's choice between the centralization or delegation of control responsibility. Indeed, management may have options which involve the erosion of some or all aspects of supervisory tasks and roles, but other options will involve the opportunity to create new roles based on the exploitation of the operational control potential of the new technology (Dawson and McLoughlin 1986). They point out that the precise form of organizational arrangements that might arise from the pursuit of management strategies are, of course, likely to be shaped and mediated by situational factors.

The study done by Millman and Hartwick (1987) suggests the presence of multiple and concurrent processes occurring during the introduction and use of IT in organizations. Moreover, they highlighted the indeterminate nature of the consequences resulting from the use of IT by suggesting that these multiple and concurrent processes are likely to have a variety of direct effects, due to greater efficiency and effectiveness of IT artifacts themselves, and indirect effects, due to the greater enrichment and satisfaction of jobs and work of users.

1990s

1. Summary of Dominant Rhetoric for this Period

The dominant rhetoric for this decade can be referred to as *interpretive structurationist* research perspective. Compared to the assumptions of a positivist perspective, interpretivism is an

epistemological position which assumes that there is no objective reality which can be discovered by researchers and replicated by others (Walsham 1993). Instead, interpretive approaches assume that knowledge of reality, including the domain of human action, is a subjective social construction by human actors (including researchers) and that our theories concerning reality provide ways of making sense of the world rather than discoveries about the world which represent absolute truth (Walsham 1993). Centered on human interpretations and social meaning, interpretive methods of research are aimed at producing an understanding of the context of the IS, and the process by which the IS influences and is influenced by its context (Walsham 1993).

An interpretive structurationist research perspective means also that this perspective is based on Giddens' structuration theory (1984). Structuration theory combines subjective and objective conceptions of organizations simultaneously through its core concept of the duality of structure, conceiving structure and human action as mutually constitutive and each being both constrained and enabled by the other (Giddens 1984). He proposes the existence of three dimensions of structures (signification, domination, and legitimation) and the concept of modalities as mechanisms to explain the mutual and indeterminate influence between structure and human agency.

2. Exemplars

Exemplar 1: Orlikowski and Robey (1991)

Orlikowski and Robey (1991) highlighted the dual nature of IT by focusing our attention on how IT shapes human action through its provision of structural opportunities and constraints

and on how IT itself is shaped by human action and prior institutional properties. As a result of this dual nature of IT, they proposed the use of structuration theory to investigate the relationship between IT and organizations. According to Orlikowski and Robey (1991), the adoption of structuration theory allows IS researchers to overcome several limitations of prior one-sided perspectives:

(i) Structuration theory assumes that structures exist only through ongoing human action thus avoiding the determinism and reification of technology proposed by objectivist theories;

(ii) Structuration theory recognizes that organizational properties can become institutionalized and assume objective identities beyond easy reach of acting individuals thus avoiding the extreme voluntarism advocated by subjectivist theories;

(iii)Structuration theory pays attention to the ongoing interactions between human action and the contextual and historical factors of social practices that produce and reproduce social systems over time; as such, it pays attention to factors that have been neglected by much of the objectivist and subjectivist research.

Moreover, Orlikowski and Robey (1991) argue that structuration theory fits the class of theory recommended by Markus and Robey (1988) for research into the interaction of information technology and organizations. Indeed, structuration theory is an emergent, process theory which accommodates multiple levels of analyses, is contextually and temporally situated, and avoids the blinders of historical accounts of social phenomena (Orlikowski and Robey 1991).

Exemplar 2: Orlikowski (1993)

Orlikowski (1993) studied the adoption and use of computer-aided software engineering (CASE) tools over time in two organizations. To make sense of the apparently inconsistent findings in the literature about the outcomes of the use of CASE tools, she proposed to shift the focus away from specific outcome expectations and to define the organizations' experiences with the adoption and use of CASE tools in terms of processes of incremental or radical organizational change. She argues that such a perspective allows researchers to anticipate, explain, and evaluate different experiences and consequences following the introduction of CASE tools in organizations. Based on these findings, Orlikowski (1993) developed a theoretical framework for conceptualizing the organizational issues around the adoption and use of these tools, thus filling a knowledge gap in the literature about CASE tools. Her framework and findings suggest that the intentions and actions of key players, the change process they enact, and the social context into which tools are implemented, critically influence what organizational changes are associated with the use of CASE tools. As such, Orlikowski (1993) proposes that in order to investigate the experiences and outcomes associated with the adoption and use of CASE tools, researchers should consider the interaction over time between the intentions and actions of key players around the technology, social context of systems development, and the implementation process followed by the organization.

3. Implications for Researchers and Practitioners

Orlikowski and Robey (1991) demonstrated clearly how a structurationist approach based on Giddens' structuration theory (1984) can benefit to IS researchers investigating the relationship between IT and organizations. Structuration theory's main strength is that it accounts not only

for the fact that structure can both constrain and enable human action but also for the mutual and indeterminate influence of structure and human agency without privileging one or the other or adopting a deterministic stance. Orlikowski (1993) demonstrated the importance for IS researchers to pay attention to the human interpretations and social meaning of IT artifacts as well as their context of use when investigating the experiences and outcomes associated with their adoption and use in organizations. As such, the interpretivist structurationist research perspective can be seen as a theoretical solution to overcome the limitations of the deterministic approaches of the 1960s and 1970s while capturing the benefits of the implementation of the emergent process perspective of the 1980s.

2000s

1. Summary of Dominant Rhetoric for this Period

This decade can be characterized by the adoption of a *human agency* research perspective. In a human agency perspective, ontological priority is given to the role of human agency over the role of social structure and technology as a determinant of the consequences resulting from the use of IT in organizations (Boudreau and Robey 2005). This research perspective is built upon the concepts of human agency and voluntarism, which stipulate that humans can exert some power and free will to influence the design, interpretation and use of technology and their environment to achieve their interests and goals (Leonardi and Barley 2008). Human agents can can vary their use of technology over time and improvise new ways of using it that produce novel and unanticipated consequences (Boudreau and Robey 2005). In a human agency perspective, technology is defined as a material artifact that is socially defined and socially produced, and thus is relevant only in relation to human agents engaging with them (Orlikowski

2010). Technology is involved in social change only at the discretion of human agents, even in presence of automated manufacturing technologies and especially with IT (Orlikowski and Barley 2001). Because users' practices, beliefs and agendas significantly shape how IT affects organizing, human agency matters even when it is unwitting (Leonardi and Barley 2008). Even in organizations where the use of IT is mandated rather than voluntary, IS research has demonstrated that users can still exercise their agency by different means such as appropriate IT in ways that were not imagined by their designers (DeSanctis and Poole 1994) selectively using or misusing the technology's functions and developing workarounds and shadow systems (Azad and King 2008; Boudreau and Robey 2005; Kallinikos 2004).

2. Exemplars

Exemplar 1: Orlikowski (2000)

Orlikowski (2000) propose to extend the structurational perspective on technology by the development of a practice lens to examine how people, as they interact with a technology in their ongoing practices, enact structures called technologies-in-practice which shape their emergent and situated use of that technology. According to her, the fact that a practice lens recognizes that the possibility to change technology structures is inherent in every use of technology allows researchers to understand when, where, how, and why people choose to reinforce, ignore, enhance, undermine, change, work around, or replace their existing structures of technology use. As such, structures of technology use are not embodied in the technology but constituted recursively as humans regularly interact with certain properties of a technology and thus shape the set of rules and resources that serve to shape their interaction (Orlikowski 2000).

Exemplar 2: Boudreau and Robey (2005)

Boudreau and Robey (2005) investigated the role of human agency in shaping the enactments of an integrated computer-based enterprise information system, assumed to constrain human action, after its implementation in a large government agency. They found that despite the organizational change agenda related to the conversion to the new system, users initially chose to avoid using it as much as possible. This initial inertia was overcome over time as a variety of stakeholders exercised social influence to change the pattern of use (Boudreau and Robey 2005). By highlighting the dynamic nature of enactment, their empirical results supported a temporal view of human agency (Emirbayer and Mische 1998). Using the concept of improvised learning, Boudreau and Robey (2005) also demonstrated how social influences from other people can produce changes in enactments of technology use over time, going from inertia to reinvention of the technology. Their results showed that even an integrated technology like an ERP system, often seen as a "hard" constraint on human agency, can be resisted and reinvented in use by human agents.

3. Implications for Researchers and Practitioners

The development of a practice lens by Orlikowski (2000) to examine how structures called technologies-in-practice are enacted in practice puts a large emphasis on the role of human agents. Indeed, her study adopts a focus on human agency and the enactment of emergent structures in the recurrent use of technologies instead of a focus on technologies and embodied structures and their influence on use. The study done by Boudreau and Robey (2005) also puts a large emphasis on the role of human agents. Their results showed how human agents can shape the enactments of technology, going from inertia to reinvention of the technology. As such,

Boudreau and Robey (2005) demonstrated that even when IT represents a "hard" constraint on human agency, human agents have still residual power to resist it and reinvent it in use.

The adoption of a human agency research perspective in the study of the relationship between IT and organizations can be seen as a longer term shift away from technological determinism toward more balanced causal arguments incorporating both agency and technological constraints (Boudreau and Robey 2005).

Discussion

In this section, we present first a summary of the results before analyzing them formally. The section concludes with the important implications drawn for future research.

Results Summary

Over the last fifty years, we have seen important shifts in the dominant theoretical perspectives adopted by IS researchers to study the relationship between IT and organizations. Early studies in the 1960s have adopted a technological determinism research perspective in which IT was treated in the same way as production technologies, as an external force producing predictable and inevitable impacts on organizations and their members. Interestingly, empirical research generated contradictory findings on almost every dimension of the hypothesized computer impacts (Markus and Robey 1988; Robey 1977).

In the 1970s, the contingency research perspective became the dominant theoretical perspective. This research perspective acknowledges the influence of additional contextual variables or

contingencies in the production of IT impacts on organizations and their members. The fact that the impacts of technology are seen as contingent on the fit with other independent variables soften deterministic predictions about IT impacts. Other theoretical research perspectives have also been adopted during time period. One example is the organizational imperative perspective, in which IT is seen as a tool for solving organizational problems, acting as the dependent variable caused by the organization's information processing needs and manager's choice about how to satisfy them given the contingencies that he needs to take into account (Markus and Robey 1988). The organizational imperative perspective assumes that human actors can design and use information systems in almost unlimited ways to satisfy organizational needs and manage their impacts with almost unlimited control by attending to both technical and social concerns (Markus and Robey 1988). The organizational imperative perspective is consistent with Pfeffer's (1982) "*intendedly rational*" perspective on action which assumes that human action is goal directed and resulting from prior free rational choices based on the evaluation of alternative courses of action or a set of consistent preferences. This decade has also seen the development of the socio-technical perspective and the political perspective.

In the 1980s, researchers such as Markus & Robey (1988) started to challenge the still dominant technological determinism research perspective and its contradictory empirical results about outcomes of IT. They proposed the adoption of an *emergent process* perspective arguing that uses and consequences of technology emerge from the ongoing, complex and unpredictable interaction of people, technology and context. Compared to the deterministic causal arguments of the previous two decades, the emergent process perspective highlights the indeterminate nature of the consequences resulting from the use of IT as it does not acknowledge a dominant cause of

change (Markus and Robey 1988). This emergent process perspective is consistent with Pfeffer's (1982) "emergent" perspective on action in organizations, in which the behavior of people and organizations emerges from a dynamic interaction of external circumstances and internal motives or interests.

In the 1990s, the dominant theoretical perspective was the *interpretive structurationist* research perspective. As an interpretivist approach, it centered on human interpretations and social meaning and was aimed at producing an understanding of the context of the IS and the process by which the IS influences and is influenced by its context (Walsham 1993). Moreover, the fact that this research perspective is based on structuration theory means that it accounts not only for the fact that structure can both constrain and enable human action but also for the mutual and indeterminate influence of structure and human agency without privileging one or the other or adopting a deterministic stance (Giddens 1984).

In the 2000s, the dominant theoretical perspective was the *human agency* research perspective. This research perspective has at its core the concepts of human agency and voluntarism, which stipulate that humans can exert some power and free will to influence the design, interpretation and use of technology and their environment to achieve their interests and goals (Leonardi and Barley 2008). Human agency can be exerted even in the presence of highly constraining environments. Technology is defined as a material artifact that is socially defined and socially produced, and thus is relevant only in relation to human agents engaging with them (Orlikowski 2010). Because users' practices, beliefs and agendas significantly shape how IT affects organizing, human agency matters even when it is unwitting.

Results Analysis

Overall, our analysis of the results suggests the following findings regarding the shifts in the dominant theoretical perspectives adopted by IS researchers to study the relationship between IT and organizations. In each of the last five decades, a new dominant theoretical perspective was developed and adopted to extend the previous decade's rhetoric by getting even further away from technological determinism in the sixties and closer to more balanced causal arguments to explain the consequences of IT on organizations and their members.

The contingency perspective in the seventies introduced the concept of contingencies defined as additional variables influencing the production of IT impacts on organizations and their members. These contingencies somewhat soften deterministic predictions about these IT impacts. The emergent process perspective in the eighties can be seen as a theoretical solution overcoming the limitations of the deterministic approaches of the 1960s and 1970s by introducing the concept of an ongoing, complex and unpredictable interaction of people, technology and context as the source of IT outcomes. By acknowledging no dominant cause of change (Markus and Robey 1988), the emergent process perspective highlighted the indeterminate nature of the consequences resulting from the use of IT.

Then, the interpretivist structurationist perspective in the nineties can be seen as a theoretical solution to better capture the benefits of the implementation of the emergent process perspective of the 1980s. The use of an interpretive lens and a structurationist approach based on Giddens' (1984) structuration theory can be seen as providing additional concepts and mechanisms

helping researchers to better understand the ongoing, complex and unpredictable interaction of people, technology and context proposed in the emergent process perspective. Finally, the human agency perspective in the 2000s can be seen as a theoretical solution to help researchers better understand conflicting IT outcomes by adopting a more voluntaristic stance which favors the role of human agency and social processes (Boudreau and Robey 2005). The concepts of human agency and voluntarism stipulate that humans can exert some power and free will to influence the design, interpretation and use of technology and their environment to achieve their interests and goals (Leonardi and Barley 2008), even in the presence of highly constraining environments. This analysis suggests also important implications for future research which are now described.

Important Implications Drawn for Future Research

Time for correction in response to agentic turn?

As a result of these developments in theoretical perspectives, theory about IS post-adoption behavior has tilted toward human agency. However, the tilt toward human agency may be seen as too severe as it somewhat neglects the influence of IT artifacts and their material aspects. By putting a large emphasis on human agency, a human agency perspective treats IT as almost indefinitely malleable and interpretively flexible. This suggests that IT post-adoption behavior is almost never seen as constrained by IT, even in the case of large integrated packages such as ERP systems (Boudreau and Robey 2005). However, this development of theory about IS post-adoption behavior is seen by a growing number of scholars as difficult to justify. Researchers such as Hutchby (2001) react against the treatment of IT as "text" that could be interpreted and manipulated in any way, and others like Volkoff et al. (2007) suggest that material aspects of technology do matter as they can both constrain and enable human action. If IS researchers

assume that material properties of IT matter in some ways, then there is a need to theorize those properties in relationship to voluntaristic human behavior, which we already know can make a difference (Leonardi and Barley 2008).

Interestingly, material aspects of technology were at the core of early research on the relationship between technology and organizations. Indeed, technology was primarily defined in terms of types of manufacturing hardware: discrete objects including equipment, machines and instruments (Orlikowski 2010). Moreover, the technological determinism perspective was already taking into account the material agency of technology by considering technology as an external force, independent of human action, producing inevitable and predictable impacts on organizations and their members.

Moreover, the increasing abstraction of the concept of technology over time may help to explain why the influence of IT artifacts and their material aspects has been neglected in the least theoretical perspectives. For instance, the concept of technology was expanded beyond production or manufacturing environments by making it more abstract so that it can also be applied to the processes and knowledge used in offices and service organizations. Moreover, technology started to be described in terms of the characteristics of tasks (e.g., complexity or predictability) that were seen to be proxies for technology (Orlikowski 2010). She explains that the abstraction of the concept of technology over time allowed for greater research generalizability by making it applicable to more types of technology and organizational settings. However, she notes that this abstraction has unfortunately led to the neglect of the specific characteristics and material aspects of technologies.

How theoretical attention to material IT artifacts can be restored in IS research?

Two approaches can be used by IS researchers for restoring theoretical attention to material IT artifacts in IS research. First, IS researchers can study materiality of IT artifacts through the use of other conceptualizations of technology. For example, IS researchers can draw on the concept of sociomateriality to study the materiality of IT artifacts. Sociomateriality is based on a relational ontology and focuses on how meanings and materialities are enacted together in everyday practices (Orlikowski 2010). She explains that according to a performative perspective of sociomateriality, technologies have no inherent properties, boundaries or meanings, but are bound up with the specific material-discursive practices that constitute certain phenomena. Since such material-discursive practices enact specific local resolutions to ontological questions of the nature of phenomena, researchers need to look at the ongoing and dynamic 'agential cuts' that perform and stabilize/destabilize particular distinctions, boundaries and properties within phenomena in practice (Orlikowski 2010). IS researchers can also study the influence of the distinctive and material aspects of IT artifacts embedded in organizational practice on the design and performance of such practice. This suggestion seems especially relevant and promising as an increasing number of organizational tasks are performed through the use of IT artifacts involved in multiple interdependent organizational processes. Such an investigation constitutes the subject of another study part of this dissertation.

Second, IS researchers can extend existing theories by incorporating concepts representing the distinctive and material aspects of IT artifacts. The extension of organizational routines theory to incorporate the influence of the distinctive and material aspects of IT artifacts constitutes the subject of another study part of this dissertation. While these approaches are likely to generate

novel insights about the relationship between IT and organizations, researchers are likely to face new challenges such as the definition and operationalization of relational concepts based on the relationship between material IT artifacts and human users, distinguishing between material aspects of IT artifacts that enable human action and those that constrain it, and theorizing about the concept of material agency.

Conclusion

This paper provided an overview of the dominant theoretical perspectives that IS researchers have used to study the influence of technology on organizations and their members in the last five decades. Without being exhaustive, our review of IS literature identified, for each decade, the dominant theoretical perspectives used in the IS field. We illustrated them by selecting and describing two exemplars published in the decade and explained their implications for researchers and practitioners. The results of this study showed that in each of the last five decades, a new dominant theoretical perspective was developed and adopted to extend the previous decade's rhetoric by getting even further away from technological determinism in the sixties and closer to more balanced causal arguments explaining the consequences of IT on organizations and their members. Our analysis suggested also important implications for future research such as the need for IS researchers to study and theorize the materiality of IT artifacts and potential approaches that IS researchers can used for restoring theoretical attention to material IT artifacts in IS research.

As with any research, our approach for this research has a number of limitations. We recognize that the identification of dominant theoretical research perspectives used in research on IT

influence on organizations and their members as well as exemplars to illustrate them is a subjective activity. Moreover, mapping them to specific time periods is not a straightforward exercise as it also involves subjectivity since IT research streams often overlap decades. Therefore, other researchers may come up with different results and conclusions. This research can be extended by the review of additional IS journals and by looking at other aspects of the relationship between IT and organizations. Finally, although IS researchers need to restore theoretical attention to material IT artifacts in IS research, they should not reproduce history by favoring materiality over human agency and adopting a deterministic stance.

References

Azad, B., & King, N. (2008). Enacting computer workaround practices within a medication dispensing system. [Article]. *European Journal of Information Systems, 17*(3), 264-278.

Boudreau, M. C., & Robey, D. (2005). Enacting integrated information technology : A human agency perspective. *Organization Science, 16*(1), 3-18.

Burlingame, J. F. (1961). Information Technology & Decentralization. *Harvard Business Review, 39*(6), 121-126.

Dawson, P., & McLoughlin, I. (1986). Computer Technology and the Redefinition of Supervision: A Study of the Effects of Computerization on Railway Freight Supervisors. *Journal of management studies, 23*(1), 116-132.

DeSanctis, G., & Poole, M. S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science, 5*(2), 121-147.

Dutta, A. (2008). A New Perspective in Understanding The Role of Information Technology Features in Technology Use Pattern. *Vikalpa: The Journal for Decision Makers, 33*(1), 55-68.

Emirbayer, M., & Mische, A. (1998). What Is Agency? *The American Journal of Sociology, 103*(4), 962-1023.

Galbraith, J. R. (1974). Organization Design: An Information Processing View. *Interfaces, 4*(3), 28-36.

Giddens, A. (1984). *The Constitution of Society: Outline of the Theory of Structuration* (Edition 1 ed.). Los Angeles: University of California Press.

Hutchby, I. (2001). Technologies, Texts and Affordances. *Sociology, 35*(02), 441-456.

Kallinikos, J. (2004). Deconstructing information packages: Organizational and behavioural implications of ERP systems. *Information Technology & People, 17*(1), 8-30.

Klatzky, S. R. (1970). Automation, Size, and the Locus of Decision of Decision Making: The Cascade Effect. *The Journal of Business, 43*(2), 141-151.

Leonardi, P. M., & Barley, S. R. (2008). Materiality and change: Challenges to building better theory about technology and organizing. *Information and Organization, 18*(3), 159-176.

Markus, M. L. (2005). Technology-shaping effects of e-collaboration technologies: Bugs and features. *International Journal of e-Collaboration, 1*(1), 1-23.

Markus, M. L., & Robey, D. (1988). Information Technology and Organizational Change: Causal Structure in Theory and Research. *Management Science, 34*(5), 583-598.

Millman, Z., & Hartwick, J. (1987). Impact of Automated Office Systems on Middle Managers and Their Work. *MIS Quarterly, 11*(4), 479-492.

Orlikowski, W. J. (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. *MIS Quarterly, 17*(3), 309-340.

Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organization Science, 11*(4), 404-428.

Orlikowski, W. J. (2010). The Sociomateriality of Organisational Life: Considering Technology in Management Research. *Cambridge Journal of Economics, 34*, 125–141.

Orlikowski, W. J., & Barley, S. R. (2001). Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other? *MIS Quarterly, 25*(2), 145-165.

Orlikowski, W., & Robey, D. (1991). Information Technology and the Structuring of Organizations. *Information Systems Research, 2*(2), 143-169.

Pfeffer, J. (1982). *Organizations and Organization Theory*. Marshfield, MA: Pitman.

Robey, D. (1977). Computers and Management Structure: Some Empirical Findings Re-examined. *Human Relations*, *30*(11), 963-976.

Volkoff, O., Strong, D. M., & Elmes, M. B. (2007). Technological Embeddedness and Organizational Change. *Organization Science, 18*(5), 832–848.

Walsham, G. (1993). *Interpreting Information Systems in Organizations*. Chichester: John Wiley & Sons.

Whisler, T. L. (1965). The Manager and the Computer. *Journal of Accountancy, 119*(1), 27-32.

How IT Artifacts Influence the Design and Performance of Organizational Routines: Extending Organizational Routines Theory

Benoit Raymond
Computer Information Systems Department
J. Mack Robinson College of Business
Georgia State University
Atlanta, Georgia USA

Abstract

For many years, research on IS post-adoption behavior has favored human agency and somewhat neglected the role of materiality of artifacts. Instead of treating IT as indefinitely malleable and interpretively flexible such as "text" that could be read in any way, we adopt a perspective in which material aspects of technology both enable and constrain human action. Using organizational routines theory as the theoretical lens, the objective of this research is to theorize how IT artifacts influence the design and performance of organizational routines. By doing so, we seek to extend this theory by offering potential solutions to overcome its main limitations, which are its neglect of the material aspect of artifacts, its failure to distinguish between the distinctive characteristics of IT artifacts and other artifacts, and its treatment of all artifacts as outside of organizational routines. We argue that artifacts can be seen as latent material agents that possess an inherent capacity to act independently of human action. The distinctive characteristics of IT artifacts increase their potential to become embedded in organizational routines and be considered as latent artifact-based structures composed of material and objective aspects and a structural potential. When embedded in organizational routines, IT artifacts acquire the capacity to play roles similar to those played by the ostensive and performative aspects of

organizational routines and act as generative systems. Based on these arguments, we treat embedded IT artifacts as integral to organizational routines, able to mediate the relationship between their ostensive and performative aspects, but also contribute to the generation of novel routine performances.

Introduction

Over the years, there has been a noticeable shift in information system (IS) research from the study of IS implementation and adoption to the study of IS post-adoption issues. This change in research focus can be explained by two main reasons. First, the acceptance and adoption of information technology (IT) in general are no longer an issue. IT is seen either as a source of competitive advantage or simply as a competitive necessity. Many organizations have made the development and use of IT their core competency and others use IT to operate on the Internet without any physical presence. IT has enabled new business models that were not possible or profitable before. Today it is not rare to observe individuals and organizations adopting new IT even if their actual benefits have yet to materialize. Second, researchers and practitioners have realized that IT initial adoption is only a first step in the process of creating business value. Whatever the technology, its success depends on its continued use so that its benefits can materialize for the organization. Similarly, negative impacts resulting from the use of IT may require time in order to be observed. IS researchers need a better understanding of the variations in IS post-adoption usage and therefore should move beyond dichotomous "adoption versus non-adoption" and account for the "missing link"—actual usage—as a critical stage of business value creation (Zhu and Kraemer 2005).

However, IS post-adoption behavior is a complex phenomenon that has strong practical and theoretical implications as it can lead to both positive and negative consequences for the organization. The outcomes of technology can be seen as indeterminate (Boudreau and Robey 2005) as even identical technologies may lead to different structural outcomes in different situations (Barley 1986; Robey and Sahay 1996). Moreover, because technology usage may vary over time as users gain first-hand experience with it (Bhattacherjee and Premkumar 2004), so may its business value. For example, in their study of EDI implementation, Morris et al. (2003) found that short-term usage of EDI was unlikely to result in significant organizational change, but long-term usage was. Measuring IS usage is not a straightforward task as many criteria can be used such as the log-in time, number of outputs produced and the number of functions used. Even technologies used on a regular basis may be used only at a superficial level. Moreover, IS usage not only concerns internal users but also external users such as business partners and clients. This brought IS researchers such as Burton-Jones and Straub (2006) to rethink the concept of IS usage.

As the successful initial adoption of technically-sound IS did not seem to guarantee the production of expected outcomes and usage over time, researchers started to look at potential factors explaining these results. A research perspective referred to as social voluntarism was introduced as a general way to explain that human agency was responsible for most of what happens after IS are implemented and initially adopted. This research perspective is built upon the concepts of human agency and voluntarism, which stipulate that humans can exert some power and free will to influence the design, interpretation and use of technology and their environment to achieve their interests and goals (Leonardi and Barley 2008). Because users'

practices, beliefs and agendas significantly shape how IT affects organizing, human agency matters even when it is unwitting. Even in organizations where the use of IS is mandated rather than voluntary, IS research has demonstrated that users can still exercise their agency by different means such as selectively using or misusing the technology's functions, and developing workarounds and shadow systems (Azad and King 2008; Boudreau and Robey 2005; Kallinikos 2004). By putting a large emphasis on human agency, voluntarist theory treats IT as almost indefinitely malleable and interpretively flexible.

As a result of these developments, theory about IS post-adoption behavior has tilted toward human agency and neglected the IT artifact. This suggests that IS post-adoption behavior is almost never seen as constrained by IT, even in the case of large integrated packages such as ERP systems (Boudreau and Robey 2005). However, this development of theory about IS post-adoption behavior is seen by a growing number of scholars as difficult to justify. Researchers such as Hutchby (2001) react against the treatment of IT as "text" that could be read in any way, and others like Volkoff et al. (2007) suggest that material aspects of technology do matter as they can both constrain and enable human action. If IS researchers assume that material properties of IT matter in some ways, then there is a need to theorize those properties in relationship to voluntaristic human behavior, which we already know can make a difference (Leonardi and Barley 2008).

Organizational routines represent an important part of almost every organization because work is usually organized and accomplished via organizational rules and processes involving multiple participants. Organizational routines are different than individual routines and interactions with a

technology as they involve multiple actors and interdependent actions which constrain individual agency. Being at the core of organizations, an effective way to better understand IS post-adoption behavior is to study the influence of IT artifacts and their material aspects on the design and performance of organizational routines, which is the objective of this study.

Understanding the material aspects of organizational routines is increasingly relevant as organizations perform core business processes by relying more heavily on large integrated software packages which embed fixed and standardized work processes and functionality that often limit users' possibilities to configure pre-defined parameters. The capacity to parameterize the software package is usually not sufficient for creating a working information system (Boudreau and Robey 2005; Kallinikos 2004; Scott and Wagner 2003). As a result, the functionality of software packages may not fully meet users' work-related needs and the design of their interfaces may not be intuitive and user-friendly.

Organizational routines theory (ORT) is an influential theory that explains both organizational stability and change by incorporating structures and human agency in its concept of ostensive and performative aspects of organizational routines (Feldman and Pentland 2003). However, this theory, in its current form, regards IT artifacts as separate from organizational routines themselves (Pentland and Feldman 2008), thus making its use to study IS post-adoption behavior more difficult. This research seeks to extend ORT by focusing on the influence of the material and distinctive aspects of IT artifacts on the design and performance of organizational routines. As such, this study responds to the call made by several IS researchers such as Volkoff et al. (2007) to pay more attention to the materiality of IT artifacts.

The structure of this paper is as follows. First, we describe organizational routines theory and motivate our decision to extend it. Second, we analyze organizational routines theory's limitations. Third, we propose new theoretical concepts as means to overcome these limitations. Finally, we discuss theoretical issues that lie beyond our contribution and could be investigated in future research.

Describing Organizational Routines Theory

Feldman and Pentland (2003) define organizational routines as repetitive, recognizable patterns of interdependent actions carried out by multiple actors. Generally associated with bureaucracies, for which organizational stability, regularity and continuity are defining features, organizational routines are traditionally described as a source of inertia, inflexibility, and even mindlessness (Feldman and Pentland 2003). However, as organizational routines need to be continuously enacted and re-enacted by their performers, they can also constitute a source of flexibility, adaptability, and change (Feldman and Pentland 2003; Pentland and Feldman 2008). Because performers of routines need to accommodate and adapt to the changing context of routines, they potentially generate a stream of variations to routine performances (Feldman and Pentland 2003). Routine performances can contribute both to organizational stability and inertia, by re-enacting the same pattern of action; and also to organizational flexibility and change, by promoting a new pattern of action. These varying routine performances represent the inherent capability of every organizational routine to generate organizational change (Feldman and Pentland 2003). This vision of organizational routines is consistent with Cohen's (2007) concept of "live" routines, which depend on actors who are capable of learning from experience and altering their behavior.

Because of their "liveliness," organizational routines can be conceptualized as generative systems that can produce varying and indeterminate outcomes depending on the circumstances.

To account for the possibility of both variability and change, Feldman and Pentland (2003) propose that organizational routines consist of two different but recursively related elements: the ostensive and performative aspects. The ostensive aspect of an organizational routine embodies the abstract or ideal nature of the routine (Feldman and Pentland 2003). This ostensive aspect acts as a structure and may be codified as a standard operating procedure or exist implicitly as a taken-for-granted norm. The ostensive aspect may also have a significant tacit component embedded in procedural knowledge (Feldman and Pentland, 2003). The performative aspect of an organizational routine consists of the actual performances of the routine by specific people, at specific times and places (Feldman and Pentland, 2003). It represents the routine in practice and is constructed from a repertoire of possible human actions that are inherently improvisational. Feldman and Pentland (2003) note that this understanding is consistent Bourdieu's (1977) theory of practice, which argues that, while practices are carried out against a background of rules and expectations, the particular courses of action chosen are always, to some extent, novel. The ostensive and performative aspects are both necessary for an organizational routine to exist, as neither aspect alone is sufficient to explain (or even describe) the properties of the phenomenon referred to as organizational routines (Feldman and Pentland 2003).

Motivating the Choice of Organizational Routines Theory

Our decision to focus on and extend organizational routines theory is motivated by an analysis of the strengths and limitations of several theories that we considered relevant for the study of IS

post-adoption behavior. Essentially, we are looking for a theory that 1) offers sufficient specificity to provide novel insights about IS post-adoption behavior, 2) takes into account the mutual influence of structure and human agency without favoring one or the other, and 3) allows for an appropriate treatment of the material and distinctive aspects of IT artifacts. By establishing these criteria, we want to avoid the use of grand theories involving abstract concepts that are difficult to operationalize in IS research. We also want to avoid theories that favor determinism or human agency as any tilt toward one or the other is likely to limit the power of the theory to explain how IT artifacts influence the design and performance of organizational routines. Finally, we are interested in theories that can help us respond to a call made by an increasing number of researchers such as Volkoff et al. (2007) for more attention to IT artifacts in IS research. Without being exhaustive, the next section presents the strengths and limitations of three candidate theories that were analyzed: structuration theory, actor-network theory, and adaptive structuration theory. Although theories about the social shaping or construction of technology (Bijker and Law 1992; Bijker and Pinch 1987; MacKenzie and Wajcman 1985; Pinch and Bijker 1984) and technology frame theory (Davidson 2002; Orlikowski and Gash 1994; Yeow and Sia 2008) specifically address technology, they were quickly ruled out because of their favoring of human agency. This tilt toward human agency is likely to limit the power of these theories to explain how IT artifacts influence the design and performance of organizational routines.

Structuration Theory

Structuration theory combines subjective and objective conceptions of organizations simultaneously through its core concept of the duality of structure, conceiving structure and human action as mutually constitutive and each being both constrained and enabled by the other.

Giddens (1984) proposes the existence of three dimensions of structures (signification, domination, and legitimation) and the concept of modalities as mechanisms to explain the mutual and indeterminate influence between structure and human agency.

Structuration theory's main strength is that it accounts not only for the fact that structure can both constrain and enable human action but also for the mutual and indeterminate influence of structure and human agency without privileging one or the other or adopting a deterministic perspective. However, a first and important limitation of structuration theory is its strong focus on human actions, thus neglecting the material aspects of structure. Structure is considered a virtual and abstract notion inseparable from human agency in that it exists only inside the realm of human action or as memory traces orienting conduct (Jones and Karsten 2008; Volkoff et al. 2007). This makes structures more difficult to observe for researchers. While structural constraints place limits upon the feasible range of options open to an actor in a given circumstance, structuration theory considers that human agents always have the possibility to do otherwise (Jones and Karsten 2008). Human agents only comply with structural constraints because they choose to, not because they are forced to.

A second limitation of structuration theory relates to the breadth of its concept of structure, which refers to the structuring or organizing properties of any social system. Not only does structuration theory fail to address technology specifically, but its broad concept of structure also makes it more difficult for researchers to study the influence of the material and distinctive aspects of IT artifacts. Volkoff et al. (2007) argue that technology's distinctive characteristics should be acknowledged in a theory of technology-mediated organizational change. Finally,

structuration theory does not indicate which dimensions of structures are primary (infrastructure), and which are secondary (superstructure) in that they arise because of the dominance of the primary one (Macintosh and Scapens 1991).

Adaptive Structuration Theory

Adaptive structuration theory (AST) suggests that organizational change may result from the mutual influence between structures embedded in advanced technologies and the social structures that emerge as people interact with these technologies (DeSanctis and Poole 1994). AST proposes the concepts of technology's structural features, spirit and appropriation to investigate this organizational change process. The social structures provided by an advanced IT can be described in two ways: the structural features of a given technology and the spirit of this set of features (DeSanctis and Poole 1994). They explain that structural features are the specific types of rules and resources, or capabilities offered and embedded in the technology and appropriated by human agents through their use of the technology. The spirit of the technology's features is the general intent with regard to values and goals underlying a given set of structural features. Spirit reflects but is not limited to the designers' intentions, as technical constraints may make it impossible to wholly realize their intents. Spirit is also not limited to the user's perceptions or interpretations of technology's features, as while technology use may indicate some of its spirit, usage is unlikely to capture all aspects. As such, the spirit of the technology can be best identified by the researcher by treating the technology as text (DeSanctis and Poole 1994). Text is created by authors who intend a certain interpretation, but the use of pre-defined words and grammar rules may make it impossible to wholly realize their intents. Moreover, text is read by readers who can understand and interpret it in different ways.

The main strength of AST is that it acknowledges the distinctive capacity of advanced IT to embed social structures which provide them with a structural or causal potential. As these embedded social structures are likely to vary across technologies, each technology is thus seen as offering a distinctive structural or causal potential. AST also acknowledges the appropriation of these embedded social structures by human agents in their use of the technology as a potential factor in organizational change. On the one hand, the influence of structure is taken into account by the fact that adaptive structurational processes triggered by technology can lead, over time, to changes in organizational rules and resources (DeSanctis and Poole 1994). On the other hand, the influence of human agency is taken into account by acknowledging that the technology is appropriated in different ways by different people. Thus, AST accounts for the variable and indeterminate impacts of technology on group and organizational outcomes as they depend upon: the structural potential of the technology (i.e., its spirit and structural features); how technology and other structures (such as work tasks, the group's internal system, and the larger organizational environment) are appropriated by users; and what new social structures are formed over time (DeSanctis and Poole 1994).

However, AST has been the subject of several critiques. Markus and Silver (2008) identify three main concerns regarding AST: 1) the underlying assumption that IT has embedded social structures, 2) the repeating decomposition problem, and 3) the conceptualization of spirit as a property of systems that is independent of structural features. The first and third concerns are the most relevant ones for this study. Regarding the first concern, because AST implies that social structures can acquire a material existence independent of human enactments because it assumes that IT can embed social structures that then become properties of the technology. Several

researchers have criticized the idea of embedded social structures (Jones 1999a; Jones and Karsten 2008) as an inaccurate appropriation of Giddens' (1984) structuration theory. As such, AST tends to minimize the potential of human agency to influence structure by giving a fixed form to social structures embedded in the technology. Regarding the third concern, the most problematic issue for researchers such as Jones (1999a) and Pickering (1995) is the conceptualization of spirit as an embedded property of a technology. Technology is a human artifact as it is built by humans. Moreover, this technology's property called "spirit" is described with human properties such as intents, goals, and values. However, the technology's spirit is independent of humans as it represents neither the designers' intentions nor the users' perceptions (Markus and Silver 2008). Important questions about the operationalization of, and the relationships between, structural features and spirit remain unanswered.

Markus and Silver (2008) address concerns about DeSanctis and Poole's concepts of structural features and spirit by redefining them as technical objects, functional affordances, and symbolic expressions. Markus and Silver (2008) argue that whether a core feature is present in a system or not matters less than how that feature is implemented technically. As such, their concept of technical objects is different from AST's concept of structural features in that the causal powers of technical objects are understood to lie not only in functionality (information processing capabilities) but also in packaging, arrangements, and appearances. Markus and Silver (2008) argue that a key aspect of structural features is functionality, that is, what the technology enables users to do with it. They propose the concept of functional affordances, which differs from the concept of structural features in that functional affordances are viewed not as properties of technologies but as relations between technology's features and users. Finally, to overcome

difficulty with the notion that intents and values are embedded properties of technology, Markus and Silver (2008) propose the concept of symbolic expressions. This concept differs from the concept of spirit in that symbolic expressions are understood as a relation between an object and a specified user group, whereas spirit is defined as a system property.

Actor-Network Theory

Actor-network theory (ANT) suggests that actors are part of networks of relationships and uses these actor-networks as the unit of analysis. ANT uses the single concept of actants to analyze both humans and non-human objects in a network, thus avoiding the need to consider one as context for the other (Tatnall and Gilding 1999). Moreover, ANT does not rely on any supposedly innate properties or predetermined characteristics of network's actants but rather assumes that their properties are defined and constituted in their relationships with other actants in the actor-network (Tatnall and Gilding 1999). Differences in actants' properties thus represent the outcome of some process of negotiation involving power relations. Because humans actants design and implement non-human actants to fulfill human objectives (Sarker et al. 2006), ANT equates the interests of an artifact to the interests that have been inscribed in it by its designers. As such, ANT sees technology as a receptacle in which human actants' interests and perspective can be inscribed and frozen.

ANT's main strength is that it grants human and non-human actants symmetrical consideration in a given network. Moreover, ANT accounts for the variable nature of technology's impacts by assuming the radical indeterminacy of actors, both individual and collective, as they are defined and interactively constituted in their relationships with other actors in the actor-network.

However, a first limitation of ANT is that it tends to favor human agency over structure. Indeed, ANT's focus on the negotiation process, a human activity, privileges human agency and somewhat neglects structure (Volkoff et al. 2007). While ANT considers artifacts as network actants, it assumes that their goal is to serve human interests. A second limitation is that, because intentions are a characteristic exclusive to humans, non-human objects and human actors do not receive symmetrical consideration. Even if we assume that technology's intentions can be equated to designers' interests that have been inscribed in the technology, ANT does not examine technology's role in negotiations and organizational changes following technology implementation (Volkoff et al. 2007). A third limitation is that because ANT treats all non-human actants in the same way, it does not account for the distinctive characteristics of IT artifacts.

Summary

While each theory has its own strengths and limitations, organizational routines theory (ORT), as mainly developed by Feldman and Pentland (2003), seems overall to be the most appropriate theory for this study. ORT has several strengths. First, it offers mechanisms to help explain the complexity involved in the accomplishment of organizational routines and how the indeterminate nature of routine performances can contribute to both organizational stability and organizational change. This is highly relevant as in almost every organization work is organized and accomplished via organizational rules and processes. Second, ORT adopts a balanced focus on both structure, represented by the ostensive aspect of organizational routines, and human agency, represented by the performative aspect of organizational routines. Thus, ORT avoids the overestimation of the ostensive aspect that can lead managers to underestimate the importance of

the adjustments and improvisations that people undertake in routine work. Together, these strengths contribute to make organizational routines theory the most appropriate theory to examine how IT artifacts influence the design and performance of organizational routines. However, we acknowledge that this theory has also limitations which are analyzed in the next section.

Limitations of Organizational Routines Theory

A first limitation of organizational routines theory relates to how it treats artifacts, especially IT artifacts, in relationship to organizational routines. Although ORT recognizes that the ostensive and performative aspects of organizational routines can be both represented and influenced by artifacts, it states that artifacts do not meet the definition of neither an organizational routine, nor its ostensive or performative aspects, and therefore treats them outside organizational routines. Researchers, such as Volkoff et al. (2007), have criticized ORT's treatment of IT artifacts because it confers a central role to human agency in the production of routine performances. As such, it neglects to take into account how artifacts, especially IT artifacts, may influence the design and performance of organizational routines. A second limitation of ORT is that it neglects the material aspects of artifacts. Volkoff et al. (2007) state that this may result from Feldman and Pentland's use of a structurationist lens, which focuses our attention on the ostensive and performative aspects of routines while neglecting their material aspects. Consequently, ORT misses the opportunity to account for the influence of the materiality of artifacts in the design and performance of organizational routines. A third limitation of ORT is that, by making no distinction between types of artifacts, it neglects the distinctive characteristics of IT artifacts (Volkoff et al. 2007). ORT considers all artifacts to be part of the broad set of physical artifacts

lying outside organizational routines (Pentland and Feldman 2005). While an information system and a letter opener are likely to present different material properties and functional affordances, ORT treats them the same way.

In this study, we adopt the the concept of functional affordances, as defined by Markus and Silver (2008), to highlight the importance of the packaging, arrangements, and appearances of artifacts' features in affecting what technology enables users to do. Moreover, because functional affordance is a relational concept involving technology features and users, it helps to explain why users may have access only to a subset of all the possibilities for human action offered by a specific technology or use it for purposes unintended by its designer. We argue that IT artifacts have distinctive material properties and functional affordances that, in turn, are likely to influence the design and performance of organizational routines. Compared to a letter opener, an important distinctive characteristic of IT artifacts is the presence of a component called software. While this software component plays an important role, it also contributes to make the material aspect of many IT artifacts more difficult to see compared to solid physical objects. A physical barrier can both constrain and enable human activity, and because it is a physical and tangible object, its material aspect can be easily recognized. Software can also both constrain and enable human activity but because it is not a physical and tangible object, it may require the user to see the program code, interact with its features or navigate through its interface to take notice of its material aspect. Moreover, the higher complexity of IT artifacts such as enterprise software programs can be seen not only in terms of its design and feature set, but also in their tight integration with multiple interdependent organizational work processes. Although this makes

knowing how to operate IT artifacts more difficult, it is also likely to make their organizational impacts more significant.

It is not a straightforward task to overcome ORT's limitations and extend the theory so that it better accounts for the distinctive material aspects and functional affordances of IT artifacts. Incorporating technology into the structurational perspective adopted by ORT poses a challenge for IS researchers as they need to account for the material nature of technology without exiling technology to a position outside the duality of structure (Jones and Karsten 2008). According to Giddens' (1984), structure is virtual and abstract and because it is instantiated only through human actions, it cannot exist independently of human action and thus have a material aspect or be embedded in an artifact. Material resources such as technology are expected to influence social practices only through the instantiated processes of structuration (Jones and Karsten 2008). As such, ORT treats the ostensive aspect of organizational routines as a virtual structure and the performative aspect of organizational routines as traces in minds of routine performers.

While this perspective may be appropriate for conceptualizing social structures that have no concrete form, it ignores the inherent materiality of technology (Jones 1999b). Although technology may be interpretively flexible to some degree, it may not be open to infinite reinterpretation (Devadoss and Pan 2007; Orlikowski 2000; Pinch 2008). Therefore, we should be specific about its material aspects and how they limit human agency (Monteiro and Hanseth 1996). In the following sections, we spell out three key extensions of ORT: (1) the treatment of IT artifacts as latent material agents; (2) the inclusion of IT artifacts as part of the generative system of organizational routines; and (3) the explanation of how IT artifacts may influence the

design and performance of organizational routines. Taken together, these extensions overcome the limitations while providing a useful theoretical lens for IS researchers interested in the study of IS post-adoption behavior.

Extending Organizational Routines Theory

IT Artifacts as Latent Material Agents

ORT considers artifacts as rigid, mindless and static. By mainly referring to flow charts, data flow diagrams, written procedures, policy statements or transaction history as examples of artifacts, ORT may have overlooked IT artifacts and their distinctive characteristics. By taking a closer look at the distinctive material properties and functional affordances of IT artifacts, they can also be seen as flexible, mindful and dynamic. We propose to consider IT artifacts as *latent material agents*, having a material existence and a capacity or potential to exert agency in their own right that are independent of human action. Several arguments contribute to support our claim.

First, we propose that IT artifacts may be seen as *flexible* as they can accommodate changes and be used in different ways by humans. According to ORT, artifacts may reflect either the ostensive aspect of a routine, as in the case of a written procedure or a policy statement, or the performative aspect of a routine, as in the case of a transaction history or tracking database (Pentland and Feldman 2008). This means that changes to the ostensive or performative aspect of organizational routines may also result in changes to artifacts representing them. However, this flexibility varies across technologies. The material aspect of some technologies may be highly flexible and malleable and its use may be optional, resulting in fewer constraints on users

(Volkoff et al. 2007). Even enterprise software programs that are tightly integrated and limit users' options can show some flexibility. This flexibility can be most easily seen during the configuration or customization of enterprise systems, when users may be able to modify the technology's parameters or add custom fields. Frequent software updates also incorporate changes to the features of the enterprise technology.

Second, we propose that IT artifacts may also be considered as mindful in some ways. For instance, IT artifacts such as expert systems may incorporate organizational rules and policies serving as criteria to analyze, judge and make decisions without human intervention or awareness. While these incorporated rules are predefined and are the result of past human actions, they represent the organization's knowledge developed over time. Moreover, an increasing number of IS are augmented with some kind of artificial intelligence such as neural networks. This provides IT artifacts with new functional affordances that allow them to analyze and learn from past decisions and results and make more complex decisions independently of human action.

Third, we propose that IT artifacts may also be seen as *dynamic* as they have the capacity to exert material agency, that is, to act independently of human action. Pickering (1995) argues that material phenomena, such as quarks or cosmic rays, exist independently of the human actors who devise the means to demonstrate their existence. He adds that scientists' attempts to construct devices to observe particular material phenomena may be seen as attempts to marshal material agency. The capacity of artifacts to exert material agency arises from their material properties existing independently of human action and can both constrain and enable human action. This

idea is consistent with Pinch's (2008) example of synthesizers in which humans put agency into and synthesizers, in turn, assert agency in enabling and constraining the sorts of music humans can make.

The presence of software in IT artifacts makes the concept of material agency even easier to perceive. Software can enable human action but also constrain it by setting limits on the range of options available to users. For instance, Volkolf et al. (2007) found that the capacity of the enterprise system to inscribe organizational elements and their relationships in the form of system-executed transactions—sets of explicitly defined steps that require specific data inputs to automatically generate specific outcomes—gives them a material aspect that prescribed much of how the routine could be performed by employees. They explain that because the material aspect of IT artifacts is concrete and specific, it is the same for everyone, and individual interpretations do not affect how transactions are performed. Pentland and Feldman (2008) found that while the software package that was adopted by the organization's employees did not alter the list of functions that needed to be performed, it changed the specific actions needed to perform these functions and redefined who could perform certain tasks. This is consistent with D'Adderio's (2008) contention that while there is always scope for human intervention, formal rules and procedures, especially when they are embedded in technological artifacts, have a more fundamental influence on rule-following than simply describing what should be done.

Moreover, although software is normally programmed by human agents in advance of the execution of programs, programs may possess the capacity to exert material agency without any human intervention, being enacted by predefined triggers such as specific times, conditions or

events. The use of programs implies that many transactions are not performed by humans but rather executed by the technology based on predefined rules or criteria for which there are no choices to be made by users (Volkolf et al. 2007). By learning about the material properties and functional affordances of an IT artifact, users discover over time how it can provide opportunities and limits on human action, that is, its material agency potential (Yamauchi and Swanson 2010). Moreover, even if users had a complete knowledge of an IT artifact's material agency potential, the outcome of material agency on human action remains indeterminate at it depends on the contextuality of this human action. For instance, since many IT artifacts are networked technologies involving multiple actors and interdependent work processes, opportunities for human action offered by an IT artifact may be constrained by the actions of others to ensure coordination between individual actions. Finally, we argue that acknowledging the capacity of artifacts to exert material agency does not mean that artifacts and human actors should be symmetrically treated as actor-network theory does.

Functional Roles That IT Artifacts May Play Once Embedded in Organizational Routines

IT artifacts used in a practice may, over time, become embedded within particular work practices (Baxter and Berente 2010; Kuutti 1996). Looking at the degree to which an IT innovation becomes deeply intertwined into practices through use, Swanson (2004) found that as firms learn by doing, they assimilate IT innovation first through experimentation and then through routinization. According to D'Adderio (2008), neglecting to include tools and artifacts in the study of routines can only provide at best a partial picture. We propose that the distinctive characteristics of IT artifacts help them to become embedded in organizational routines. In turn, we propose that, once embedded in organizational routines, IT artifacts can play roles that are

similar to those that can be played by the ostensive and performative aspects of organizational routines as described by Feldman & Pentland (2003) and presented in Table 1.

Table 1. Comparison of functional roles that may be played by the ostensive and performative aspects of organizational routines and embedded IT artifacts

Ostensive aspect of organizational routines	Performative aspect of organizational routines	IT artifacts embedded in organizational routines
Guiding		Guiding
Accounting		Accounting and Legitimating
Referring		Referring
	Creation	Enabling
	Modification	

First, IT artifacts embedded in organizational routines can play a *guiding* role for human action in organizational routines. Because organizational elements such as work processes, data, roles and the relationships between them can be inscribed in software, embedded IT artifacts can serve as a guide or template for human action by influencing what actions ought to be taken (Feldman and Pentland 2003). This guiding role is often associated with a constraining role since the creation and enforcement of routines is considered as a primary mechanism for management to control work (Feldman and Pentland 2003). Managers hope that these artifacts will not only shape the ostensive aspect of a routine, but also constrain its performative aspect in some desirable way by narrowing the range of actions taken to ensure the reproduction of particular patterns of action (Pentland and Feldman 2008). IT artifacts embedded in routines provide managers with additional tools to constrain human agency of their employees, monitor organizational routine performances and enforce compliance. Material properties and functional affordances of embedded IT artifacts can act as a limit or boundary to human agency. Volkoff et al. (2007) found that employees had to perform their work according to the organizational elements' material aspect which was embedded in the enterprise system. By selecting, configuring and mandating the use of a specific enterprise software program, managers may

ensure the reproduction of particular patterns of action by narrowing the range of actions taken, thus enforcing a particular vision of the ostensive aspect of organizational routines and reducing the autonomy and discretion of their employees (Bansler and Havn 2004; Feldman and Pentland 2003; Pentland and Feldman 2008).

Software may also make information more visible across an organization thus making it easier to control that actions actually comply with the software (D'Adderio 2008). Elmes et al. (2005) use the concept of panoptic empowerment to refer to the greater visibility of information provided by the common shared database of an enterprise system that empowers workers to do their work more efficiently and effectively, but which also makes them more visible to others throughout the organization who can then more easily exercise process and outcome control. In addition, the fact that IT artifacts are often networked technologies means that individual human actions are constrained by the actions of other users. Enterprise software programs that integrate interdependent work processes become the mediators of this constraining role as they enforce the appropriateness of users' interactions with the system to ensure conformity and consistency across processes. While practitioners can often choose to bypass the software, their boycott will hold consequences for them in terms of their ability to have their actions or feedback taken into account by others in the organization (D'Adderio 2008). However, a guiding role does not determine human action as details of routine performances always remain open to human choice (Feldman and Pentland 2003). In fact, this guiding role played by IT artifacts embedded in organizational routines may also enable human action in organizational routines. This enabling role may be best associated with the performative aspect of organizational routines which is described later.

Second, embedded IT artifacts can play *accounting* and *legitimating* roles in organizational routines. The focus of the *accounting* role is on providing a retrospective record for actions already taken. As in the case of black box flight recorders in airplanes, IT artifacts embedded in organizational routines may help to describe and explain past interactions with a technology. The focus of the *legitimating* role is on justifying routine actions as established, institutionalized norms of conduct (Feldman and Pentland 2003). We propose that, once embedded in organizational routines, IT artifacts can serve as structures of legitimation by justifying and lending a sense of appropriateness to particular actions while identifying and preventing illegitimate actions. As defined in structuration theory (Giddens 1984), structures of legitimation are codes, normative rules, moral obligations and values involved in the moral constitution of social action: in other words, the institution's "collective conscience" or "moral consensus" (Macintosh and Scapens 1991). We argue that IT artifacts have the capacity to embed organizational codes, values and norms in the technology, thus materially influencing human action. Support for this argument resides in Gosain's (2004) use of institutional theory to explain how enterprise systems become objects of an institutionalization process during system configuration and later become media for carrying the institutional logic during use. For example, IT artifacts can embed and thus promote a culture of discipline, rigor and precision. Volkoff et al. (2007) also found that an enterprise system implicitly embedded sanctions by making interactions or data that were inconsistent with system-embedded work practices highly visible and difficult to correct. This culture embedded in the IT artifact eventually influenced users as they recognized that the technology only worked smoothly when they performed their work routines with strict discipline (Volkoff et al. 2007). Elmes et al. (2005) use the concept of

reflective conformity to describe how the integrated nature of the enterprise system with its embedded rules and procedures for organizational processes leads to greater employee discipline while simultaneously requiring them to be highly reflective as well in order to achieve organizational benefits from the enterprise system.

Third, embedded IT artifacts can play a *referring* role for human action in organizational routines. The focus of this role is on allowing performers of routines to execute their specific work-related tasks and make sense of a sea of interdependent activities without being fully aware of all the details involved that could otherwise be overwhelming (Feldman and Pentland 2003). For instance, just as a production line worker only has to learn work processes related to his or her workstation, users of enterprise software programs have only to learn and understand the subset of technology's features related to their tasks. Yamauchi and Swanson (2010) call this referring aspect of software as the "familiarity pocket" within which system users understand specific features and functions while ignoring others. Thus, IT artifacts embedded in organizational routines can serve as a gloss, an abstract that summarizes and omits some details thus helping users to pay attention to a comprehensible and manageable portion of the entire set of technology features and organizational activities (Feldman and Pentland 2003).

Fourth, as argued earlier, the material properties and functional affordances of embedded IT artifacts may play an *enabling* role for human action in organizational routines. As latent material agents, IT artifacts embedded in organizational routines may contribute to the production of novel routine performances by altering the potential repertoire of technology's enactments. Moreover, the fact that IT artifacts embedded in organizational routines are involved

in multiple interdependent work processes helps to make these novel routine performances more visible and enduring. This is consistent with Feldman and Pentland's argument that the generation of novel routine performances that are visible or recognizable can influence the future direction of a routine. Embedded IT artifacts can also play an enabling role as what Giddens (1984) calls *allocative resources*, which refer to the capacity to harness physical artifacts, including the knowledge to operate them and thus command material objects and goods. Physical artifacts include machines, ships, and weapons as well as more abstract resources such as intelligence networks (Macintosh and Scapens 1991). By extension, knowing how to operate IT artifacts embedded in organizational routines grants more knowledgeable users a valuable power to enact them and perform organizational routines in novel ways. This perspective helps to explain why, compared to a letter opener, IT artifacts such as enterprise software programs are more difficult to harness but likely to offer more possibilities and foster power to users who know how to operate them.

These extensions to organizational routines theory demonstrate how the same functional roles proposed by Feldman and Pentland (2003) can be applied to IT artifacts that are embedded within organizational routines. The presence of IT artifacts directly affects the extent and nature of organizational routines by affecting these functional roles. These extensions thus fall comfortably within the present formulation of the theory, as Pentland and Feldman (2008) acknowledge that artifacts may influence and be influenced by organizational routines. Our extension amounts to a more detailed specification of IT artifacts' link to functional roles. By contrast, the following section presses beyond the confines of existing theory by explaining how

IT artifacts can be included within the confines of the generative system defined as an organizational routine.

IT Artifacts as Part of the Generative System

In Figure 1, we propose a process model explaining how novel enactments of embedded IT artifacts may contribute to the production of varying and indeterminate routine performances that are characteristics of a *generative system*. In this process model, IT artifacts' latent material agency contributes to the production of novel enactments of embedded IT artifacts by altering the material repertoire of technology's enactments. In turn, these novel enactments of embedded IT artifacts contribute to the production of routine performances that may translate into new patterns of organizational action. If considered legitimate, these new patterns of action may create enduring change to the ostensive aspect of the organizational routine. However, while the capacity of IT artifacts embedded in organizational routines to contribute to the generative system exists independently of human action, the actual influence of IT artifacts to the generative system is interdependent with the role of human agents. Indeed, as argued earlier, the artifacts' material agency potential exists and can be exercised independently of human action. However, its influence on human action is latent, activated only through human enactments. This idea is consistent with Pentland and Feldman's statement (2008) that the range of possible artifact's enactments is limited both by features of the artifact and by features of the social context in which the artifact is enrolled. For example, while the material repertoire of enactments for a specific technology is constant across different social contexts, using a desktop computer as a plant stand is likely to imply different constraints and opportunities for technology's enactments

than using this same desktop computer for browsing the web. Each step of this process model is now further explained.

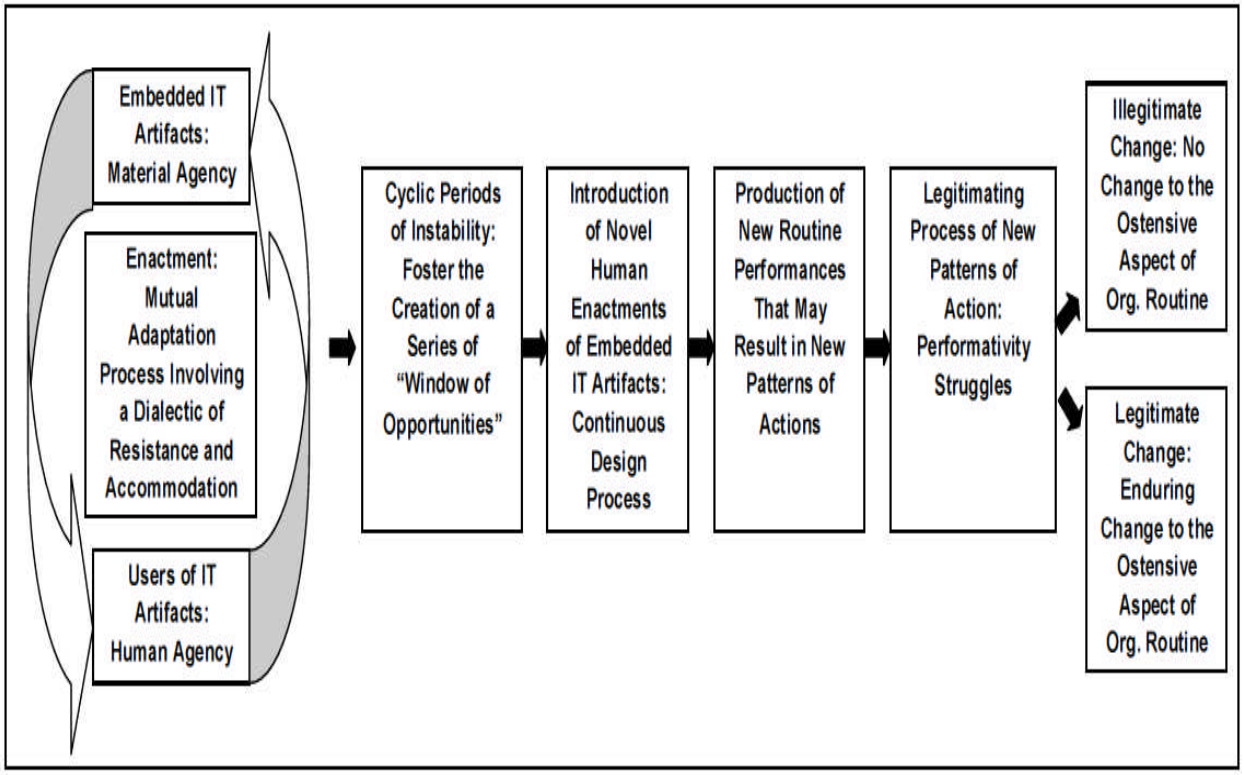

Figure 1. Process Model Explaining How Embedded IT Artifacts Contribute to the Generative System Defined as Organizational Routine

Mutual Adaptation Process between Human and Material Agencies

The introduction of new IT artifacts is not a plug-and-play type of process and continues long after their implementation, adoption, and adaptation as they must often interface with stakeholders' knowledge and interests and with technologies that are already embedded in existing practices (Baxter and Berente 2010). Artifacts are appropriated through a process of mutual adaptation whereby both the artifact and the local practices engage in cycles of change and adaptation toward eventual but temporary alignment and stabilization (Jones 1999a; Orlikowski 1996; Pickering 1995; Tyre & Orlikowski 1994). Baxter and Berente (2010) observed a high degree of tension between a well-established set of institutionalized work

processes and the demand for an artifact to achieve specific organizational goals. This mutual adaptation process between the IT artifact and work practices is represented in Figure 1 as a dialectic of resistance and accommodation between human and material agencies that occurs with each enactment of an IT artifact embedded in an organizational routine and eventually results in their temporary alignment and stabilization.

Features of IT artifacts may suggest specific technology's enactments and forbid others. In encountering resistance when they attempt to marshal material agency, human actors adopt strategies of accommodation or reconciliation practices, such as revising goals, intentions, or practices, or adjusting technological parameters (Baxter and Berente 2010). Novel technology enactments may result from the introduction of new features that users must comply with or from the development of workarounds by users (Azad & King 2008; Boudreau & Robey 2005). Therefore, novel enactments of embedded IT artifacts may occur deliberately or not, as users discover the technology's repertoire of possible enactments over time, and thus its opportunities and constraints for human action. More knowledgeable users can better exploit this repertoire of technology's enactments, including enactments that differ from what the technology's designers had in mind when it was first conceived.

Creation of a Series of "Windows of Opportunity"

Because the interactive alignment and stabilization between human and material agencies are only temporary, the continuous use of an IT artifact embedded in an organizational routine is characterized by periods during which human and material agencies are aligned and stabilized and periods during which they are not. These two types of periods alternate with each other to

form a cycle. We propose that the cyclic periods of instability between human and material agencies foster the creation of a series of "windows of opportunity" (Tyre and Orlikowski 1994) for introducing novel enactments of the embedded IT artifact. Because these periods of instability are cyclic, these novel enactments may occur as long as the IT artifact is used. As such, users can be seen as engaging in a continuous process of design through their particular appropriations of the technology in use that does not stop at some "design" stage when structure is locked into the technology (Baxter and Berente 2010; Orlikowski 1996). In turn, these novel enactments of embedded IT artifacts may generate new organizational routine performances. However, despite opportunities for new routine performances introduced by novel enactments of embedded IT artifacts, most of the time patterns of organizational action will remain the same, thus promoting organizational stability. To translate into enduring change in the patterns of action, new routine performances need not only to be recognizable, legitimate and consistent with the other interdependent activities involved in the organizational routine, but also adopted collectively by routine performers. Because IT artifacts embedded in organizational routines are involved in multiple interdependent work processes, they may contribute to make new organizational routine performances more visible and recognizable. However, artifacts that can enable or constrain individual actions may be less effective in changing collective actions (Pentland and Feldman 2008).

Legitimating Process of New Patterns of Action

Changes made to patterns of action will not automatically be reflected in the ostensive aspect of the organizational routine. In the process model depicted in Figure 1, we propose that changes to patterns of action will go through a process in which only legitimate changes will be reflected in

the ostensive aspect of the organizational routine. This legitimating process, through which a new version of the ostensive aspect emerges, involves performativity struggles resulting from the tension between competing performative programs or "agencements" promoted by different stakeholders that aim at constructing the process in different manners (D'Adderio 2008). As such, turning exceptions into rules (Feldman and Pentland 2003) may depend on the relative power and position of those who engage routines, as well as their experience with, confidence in, and intentions for the routines (Howard-Grenville 2005). Often, variations in the accomplishment of organizational routines will be seen as evidence of resistance from routine performers, considered as illegitimate changes and thus not reflected in the ostensive aspect of the organizational routine. However, the ability to improvise effective variations may also be seen as a valued skill, allowing users to overcome IT artifact's limitations or manage unexpected contingencies and exceptions (Feldman and Pentland 2003). This helps to explain why computer workarounds developed by users may become legitimate and thus reflected in the ostensive aspect of organizational routines. Describing computer workarounds as situated practices enacted through an alternate negotiated order (tacit or explicit), Azad & King (2008) found that social and collective action involved in workarounds may follow a repetitive pattern and be seen as almost routine. Now that we have explained how IT artifacts embedded in organizational routines contribute to the generative system defined as organizational routine, we explain in the next section how such IT artifacts may influence the design and performance of organizational routines.

Influence of IT Artifacts on the Design and Performance of Organizational Routines

Organizational routines theory's arguments for treating artifacts outside organizational routines may be suitable for rigid, mindless and static artifacts such as flow charts and data flow diagrams. However, we argue that these arguments may be less applicable to IT artifacts that have distinctive characteristics and become embedded in organizational routines. We propose in Figure 2 to distinguish between artifacts that are embedded in organizational routines and those that are not. We recognize that many artifacts will not become embedded in organizational routines and propose to consider these non-embedded artifacts as *accessory artifacts* and treat them outside organizational routines as ORT currently does. In contrast, we argue that some artifacts may become embedded in organizational routines and propose to consider them as *embedded artifacts* and treat them as an integral part of organizational routines. Moreover, we argue that, compared to other types of artifacts, the distinctive characteristics of IT artifacts make them more likely to become embedded in organizational routines. Overall, this theoretical treatment is consistent with Volkoff et al. (2007) who state that IT artifacts are different from other types of artifacts because they are an integral part of organizational routines and not just part of the context within which routines are executed.

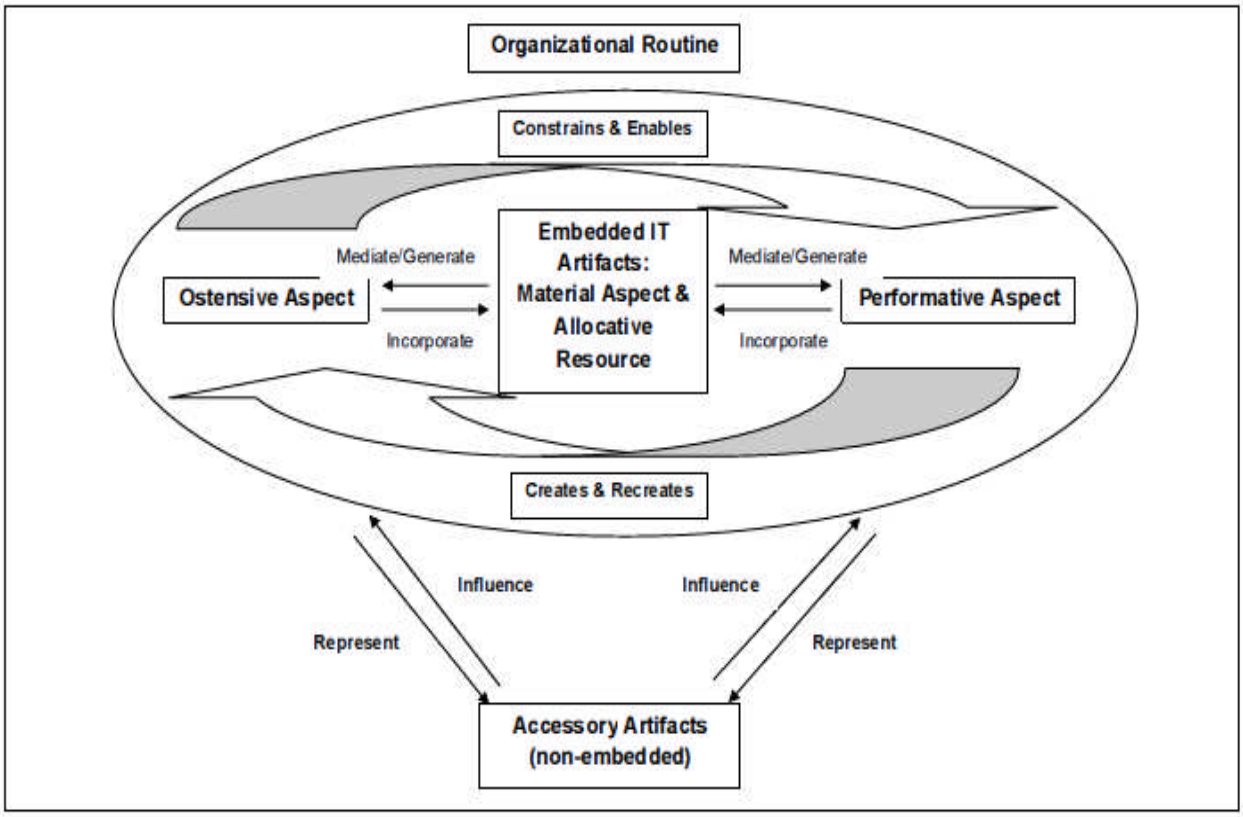

FIGURE 2. Influence of IT Artifacts on the Design and Performance of Organizational Routines (Adapted from Pentland and Feldman 2008)

We also propose in Figure 2, adapted from Pentland and Feldman 2008, that IT artifacts, when embedded in organizational routines, can influence the design and performance of organizational routines by playing two types of overarching roles. First, IT artifacts embedded in organizational routines can play a *mediating role* in the recursive relationship between the ostensive and performative aspects of organizational routines. This idea is consistent with the performative view proposed by D'Adderio (2008) in which rule-following is characterized as a typically artifact-mediated activity. Two factors contribute to make this mediating role possible. The first factor is that, as argued earlier, IT artifacts embedded in organizational routines can play roles that are similar to those played by the ostensive and performative aspects of organizational routines. The second factor is that when organizational elements are inscribed in IT artifacts,

they acquire a material aspect that interacts with and affects their ostensive and performative aspects (Volkoff et al. 2007). This mediating role is likely to gain importance as an increasing proportion of organizational routines are performed through the use of IT artifacts embedded in organizational routines such as enterprise software programs.

Second, IT artifacts embedded in organizational routines can play a *generative role* in the recursive relationship between the ostensive and performative aspects of organizational routines. As argued earlier, latent material agency of embedded IT artifacts, when materialized through technology's enactments by users, may alter the material repertoire of technology's enactments thus contributing to the generation of varying and indeterminate routine performances that are characteristics of generative systems. Moreover, we have argued earlier that IT artifacts embedded in organizational routines can act as *allocative resources,* granting the knowledgeable user valuable power to enact technology and perform organizational routines in novel ways. However, just as the influence of artifacts' material agency on human action is latent, the influence of embedded IT artifacts on the design and performance of organizational routines can also be seen as latent*,* deferred until it is activated through human interactions with the technology. Moreover, this influence is *indeterminate* due to dependence on multiple contingent factors as discussed earlier and represented in Figure 1. As such, IT artifacts embedded in organizational routines represent only one potential source of influence on the design and performance of organizational routines among others.

Taking a closer look at the materiality and distinctive characteristics of IT artifacts provides insights about how to incorporate the materiality of technology into the structurational

perspective adopted by ORT. One way is to treat IT artifacts embedded in organizational routines as what Giddens' structuration theory (1984) call *material constraints*, arising from the limitations of the material aspect of artifacts (Devadoss and Pan 2007). Building on the material constraints idea, we propose to extend it to include material properties of social systems, such as organizational routines, that can enable and constrain action. Another way, more challenging, is to treat IT artifacts embedded in organizational routines not as mere material constraints arising from the limitations of their material aspect, but as *structures* part of the various organizational, social, physical and cognitive structures that constrain and enable organizational routines (Pentland and Rueter 1994). Indeed, Giddens' structuration theory (1984) clearly distinguishes between *material constraints*, which have a material aspect, and *structures* which refer to the set of rules and resources instantiated through human action, and therefore, do not exist independently of human action. Giddens acknowledges (1984, p. 33) that some forms of allocative resources (e.g. land, raw materials etc.) have a real existence if existence is defined as a "time-space" presence. But he points out that their "materiality" does not affect the fact that such phenomena become resources . . . only when incorporated within processes of structuration. Orlikowski (2000) explains that when elements such as procedures, stored data, and public display screens become inscribed properties of a technology, they are external to human action, and as such, constitute neither rules nor resources, and thus cannot be seen to be structures. As such, structuration theory suggests that the materiality of artifacts make them external to human action and thus artifacts cannot be considered as structures. However, Pinch (2008) argues that while the duality of structure and agency, and cognition and practice has been fruitfully applied to many features of organizations, it must also be extended to the material realm. He adds that

since the social world is a world built of things and social action is through and through mediated by materiality, social theory will remain impoverished unless it addresses this materiality.

We propose to consider IT artifacts embedded in organizational routines as *latent artifact-based structures.* We posit that IT artifacts embedded in organizational routines have not only objective and material aspects but also possess, through their material agency, a structural capacity or potential that is inherent and exist independently of human action. While material agency can be exerted independently of human action as argued earlier, its actual influence on human action, whether enabling or constraining it, is latent, waiting to be discovered and deferred until activated through human enactments of the technology. Therefore, IT artifacts embedded in organizational routines can be seen as both autonomous entities able to exert material agency independently of human action and latent rules and resources for human action. Several arguments seem to support our claim.

Regarding the issue of whether artifacts can incorporate a structural potential, the concept of technology-based structures in AST (DeSanctis and Poole 1994) acknowledges that the inscription of structural features and spirit within the technology gives technology a structural or causal potential to be enacted during human interactions with the technology. Volkoff et al. (2007) state that the inscription of organizational elements in the technology, such as work processes, data and roles, happens prior to use and gives them a material aspect which is different from both the ostensive and performative aspects of organizational routines. They view enterprise systems as a source of structural conditioning that is relatively independent and enduring, existing materially in the real domain, rather than primarily as a malleable structure,

existing only empirically at the moment of instantiation. Devadoss and Pan (2007) argue that IT artifacts such as enterprise systems may create a structural constraint by imposing limits in interpretive flexibility through integrated, multiple and sometimes contradictory structures.

Regarding the issue of whether structures can exist outside human action, Orlikowski (2000) state that until such time as technological artifacts are actually used in some ongoing human action—and thus become part of a process of structuring—they are, at best, potential structuring elements, and at worst, unexplored, forgotten, or rejected bits of program code and data cluttering up hard drives everywhere. However, the concepts of reification and facticity in Giddens' structuration theory (1984) help explain how structures, such as organizations, may appear as objective and having an existence on their own. According to Giddens' structuration theory (1984), organizations represent a composite of multiple structures informed by the environment in which they are enacted and reified through their repeated enactment and thus do not exist outside the enactment of structures by its members (Devadoss and Pan 2007). Reification refers not to "thing-like" connotation, but to the facticity with which social phenomena confront individual actors in such a way as to ignore how structures are produced and reproduced through human agency (Giddens 1984, p. 180). As such, the embedding process of artifacts in organizational routines can be seen as playing a role similar to the reification process in Giddens' structuration theory (1984). However, compared to organizations, IT artifacts have distinctive characteristics as argued earlier. Because of these distinctive characteristics, we argue that the repeated enactments of IT artifacts embedded in organizational routines produces reified *latent artifact-based structures* that have a higher level of facticity, thus further contributing to make them appear as objective and having an existence on their own. This

is consistent with Devadoss and Pan's contention (2007) that IT artifacts such as enterprise systems confront users with such facticity as to create opacity of action for them.

Moreover, Feldman and Pentland (2003) state that the subjective acts of guiding, accounting, and referring and our subjective perceptions of the various aspects of organizational routines as mutually constitutive and inseparable help to create an apparently objective and concrete reality. Since IT artifacts embedded in organizational routines can play roles similar to those of the ostensive and performative aspects of organizational routines as argued earlier, and an increasing proportion of organizational routines are performed through the use of embedded IT artifacts such as enterprise software programs, we propose that aspects of organizational routines become so intrinsically associated with embedded IT artifacts that they may be seen as objectified instantiations of both the ostensive and performative aspects of organizational routines.

Conclusion

The objective of this research was to contribute to theory in the area of IS post-adoption behavior by theorizing how IT artifacts influence the design and performance of organizational routines. We first motivated our decision to focus on and extend organizational routines theory. Then, we looked at organizational routines theory's main limitations and proposed new concepts and models to extend the theory by looking at the materiality and distinctive characteristics of IT artifacts as well as the roles that they can play once embedded in organizational routines. Supported by the development of new concepts and models, we proposed three key extensions to ORT.

First, we proposed to consider artifacts as latent material agents, possessing a potential to exert material agency that exist independently but is only activated through human enactments of the technology. We explained that, compared to other types of artifacts, IT artifacts have distinctive characteristics such as their tight integration with multiple interdependent organizational work processes and the presence of software capable of incorporating organizational elements, which help them to become embedded in organizational routines. Second, we developed a process model (Figure 1) explaining how material agency of IT artifacts can alter the repertoire of technology's enactments and thus contribute to the production of varying and indeterminate routine performances which are characteristics of generative systems. Third, we proposed a new model (Figure 2), adapted from Pentland and Feldman (2008), that describes the various elements and relationships involved in organizational routines. This new model acknowledges that IT artifacts can become embedded in organizational routines, thus becoming an integral part of these routines and able to influence their design and performance by playing mediating and generative roles and acting as an allocative resource in the recursive relationship between their ostensive and performative aspects.

These contributions add clarity to recent efforts to include materiality within theoretical explanations of organizational structures, process, and change (D'Adderio 2008; Leonardi and Barley 2008; Orlikowski and Scott 2008; Pinch 2008; Volkoff et al. 2007). The desire to restore materiality to organization theory is growing, along with the ubiquitous nature of IT artifacts, thus prompting their inclusion in theoretical explanations. Instead of excluding artifacts from the definition of organizational properties such as routines, we seek to integrate the materiality of artifacts within those properties. Our approach is to maintain a conceptual distinction between

artifacts and social concepts such as human agency rather than to treat them either as inseparable "sociomaterial practices" (Orlikowski and Scott 2008) or as equivalent "actants" as in actor-network theory (Tatnall and Gilding 1999). Our theoretical approach shows how IT artifacts in particular may play a central rather than peripheral role in the design, performance and change of organizational routines.

An obvious limitation of this research is that the concepts and models as well as the arguments proposed to support them have not been empirically tested. This must be done in order to validate the extensions of ORT that we propose. Future research could investigate of how different types of IT artifacts, offering different characteristics and thus different opportunities and constraints on human action, influence the design and performance of organizational routines. Moreover, Volkoff et al. (2007) state that organizational change can result from the generation of second-order effects resulting from the interactions between organizational elements that are embedded in technology and those that are not. Future research can investigate whether our extension of organizational routines to include embedded IT artifacts provides an adequate mechanism for understanding these second-order effects.

References

Azad, B., and King, N. (2008). Enacting computer workaround practices within a medication dispensing system. *European Journal of Information Systems, 17*(3), 264-278.

Bansler, J. P. and Havn, E. (2004). Exploring the role of networks in IT implementation: The case of knowledge repositories. *Information Technology & People, 17*(3), 268-285.

Barley, S. R. (1986). Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments. *Administrative Science Quarterly*, *31*(1), 78-108.

Baxter, R.J., and Berente, N. (2010).The process of embedding new information technology artifacts into innovative design practices. *Information and Organization, 20*(3-4), 133-155.

Bhattacherjee, A., and Premkumar, G. (2004). Understanding changes in belief and attitude toward information technology usage: a theoretical model and longitudinal test. *MIS Quarterly, 28*(2), 229–254.

Bijker, W. E., and Law, J. (1992). Shaping Technology/Building Society: Studies in Sociotechnical Change, MIT Press, Cambridge, MA.

Bijker, W. E., and Pinch, P. (1987). "The Social Construction of Facts and Artifacts," in The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology, W. E. Bijker, T. Hughes, and T. Pinch (eds.), MIT Press, Cambridge, MA.

Boudreau, M-C., and Robey, D. (2005). Enacting Integrated Information Technology: A Human Agency Perspective. *Organization Science, 16*(1), 3-18.

Bourdieu, P. (1977). Outline of a Theory of Practice (Edition 1 ed.). Cambridge University Press, Cambridge. 249 p.

Burton-Jones, A. and Straub Jr, D. W. (2006). Reconceptualizing system usage: an approach and empirical test. *Information Systems Research, 17*(3), 228-246.

Cohen, M.D. (2007). Reading Dewey: Reflections on the Study of Routine. *Organization Studies*, *28*(5), 773-786.

D'Adderio, L. (2008). The performativity of routines: Theorizing the influence of artefacts and distributed agencies on routines dynamics. *Research Policy, 37*(5), 769-789.

Davidson, E.J. (2002). Technology Frames and Framing: A Socio-Cognitive Investigation of Requirements Determination. MIS Quarterly, 26(4), 329-358.

DeSanctis, G., & Poole, M. S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science, 5*(2), 121-147.

Devadoss, P., & Pan, S. L. (2007). Enterprise Systems Use: Towards a Structurational Analysis of Enterprise Systems Induced Organizational Transformation. Communications of the Association for Information Systems, 19, 352-385.

Elmes, M.B., Strong, D.M., and Volkoff, O. (2005). Panoptic empowerment and reflective conformity in enterprise systems-enabled organizations. *Information and Organization, 15*(1), 1-37.

Feldman, M. S., and Pentland, B. T. (2003). Reconceptualizing Organizational Routines as a Source of Flexibility and Change. *Administrative Science Quarterly, 48*(1), 94-118.

Giddens, A. (1984). The Constitution of Society. University of California Press, Berkeley. 402 p.

Gosain, S. (2004). Enterprise information systems as objects and carriers of institutional forces: The new iron cage? *Journal of the Association for Information Systems*, *5*(4), 151–182.

Howard-Grenville, J. A. (2005). The Persistence of Flexible Organizational Routines: The Role of Agency and Organizational Context. *Organization Science, 16*(6), 618-636.

Hutchby, I. (2001). Technologies, Texts and Affordances. *Sociology, 35*(2), 441-456.

Jones, M. (1999a). Information Systems and the Double Mangle: Steering a Course Between the Scylla of Embedded Structure and the Charybdis of Strong Symmetry, in: *Information*

Systems: Current Issues and Future Changes: IFIP, T. J. Larsen, L. Levine and J.I. DeGross (eds.), Laxenburg, Austria, 287-302.

Jones, M. (1999b). Structuration theory. In: *Rethinking Management Information Systems: An Interdisciplinary Perspective* W. Currie and B. Galliers (eds.), Oxford University Press, New York, NY, 103–135.

Jones, M. R. and Karsten H. (2008). Giddens's Structuration Theory and Information Systems Research. *MIS Quarterly, 32*(1), 127-157

Kallinikos, J. (2004). Deconstructing information packages: Organizational and behavioural implications of ERP systems. *Information Technology & People, 17*(1), 8-30.

Kuutti, K. (1996). Activity Theory as a Potential Framework for Human-Computer Interaction Research. In B. Nardi (Ed.), Context and Consciousness. Cambridge: MIT Press.

Leonardi P. M. and Barley, S. R. (2008). Materiality and change: Challenges to building better theory about technology and organizing. *Information and Organization, 18,* 159–176

MacIntosh, N. B., & Scapens, R. W. (1991). Management accounting and control systems: A structuration theory analysis. *Journal of Management Accounting Research, 3*, 131-158.

MacKenzie, D., and Wajcman, J. (1985). The Social Shaping of Technology, Open University Press, Milton Keynes.

Markus, M.L., and Silver, M.S. (2008). A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit. *Journal of the Association for Information Systems, 9*(10), 609-632.

Monteiro, E., and Hanseth, O. (1996). Social shaping of information infrastructure: On being specific about the technology. in *Information Technology and Changes in Organizational*

Work. W. J. Orlikowski, M. Jones, R. J. I. DeGross (eds.), Chapman & Hall, London, UK, 325–343.

Morris, D., Tasliyan, M. and Wood, G. (2003). The Social and Organizational Consequences of the Implementation of Electronic Data Interchange Systems: Reinforcing Existing Power Relations or a Contested Domain? *Organization Studies 24*(4), 557–574.

Orlikowski, W. J., and Gash, D. (1994). Technological Frames: Making Sense of Information Technology in Organizations. *ACM Transactions on Information Systems, 12*(2), 174-207.

Orlikowski, W. J. (1996). Improvising Organizational Transformation Over Time: A Situated Change Perspective. *Information Systems Research, 7*(1), 63-92.

Orlikowski, W.J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. *Organization Science, 11*(4), 404-428.

Orlikowski, W. J. (2007). Sociomaterial Practices: Exploring Technology at Work. *Organization Studies, 28*(09), 1435–1448.

Orlikowski, W.J., and Scott, S.V. (2008). Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals*, *2*(1), 433–474.

Pentland, B.T., and Feldman, M.S. (2005). Organizational routines as a unit of analysis. *Industrial & Corporate Change, 14*(5), 793-815.

Pentland, B. T., and Feldman, M. S. (2008). Designing routines: On the folly of designing artifacts, while hoping for patterns of action. *Information and Organization, 18*(4), 235-250.

Pentland, B.T., and Rueter, H.H. (1994). Organizational Routines as Grammars of Action. *Administrative Science Quarterly, 39*(3), 484-510.

Pickering, A. (1995). The Mangle of Practice: Time, Agency and Science (Edition 1 ed.). University of Chicago Press, Chicago. 281p.

Pinch, T., and Bijker, W.E. (1984). The Social Construction of Facts and Artefacts : Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social studies of science, 14*(3), 399-441.

Pinch, T. (2008). Technology and Institutions: Living in a Material World. *Theory and society*, *37*(5), 461-483.

Robey, D., and Sahay, S. (1996). Transforming Work through Information Technology: A Comparative Case Study of Geographic Information Systems in County Government. *Information Systems Research*, 7(1), 93-110.

Sarker, S., Sarker, S. and Sidorova, A. (2006). Understanding Business Process Change Failure: An Actor-Network Perspective. *Journal of Management Information Systems, 23*(1), 51-86.

Scott, S.V., and Wagner, E.L. (2003). Networks, negotiations, and new times: the implementation of enterprise resource planning into an academic administration. *Information and Organization, 13*, 285-313.

Swanson, E. B. (2004). How is an IT Innovation Assimilated. In B. Fitzgeral, & E. Wynn (Eds.), IT Innovation for Adaptability and Competitiveness: 267-287. Boston, MA: Springer.

Tatnall, A., and Gilding, A. (1999). Actor-Network Theory and Information Systems Research. Proceedings of 10th Australasian Conference on Information Systems: 955-966.

Tyre, M. J., and Orlikowski, W. J. (1994). Windows Of Opportunity - Temporal Patterns Of Technological Adaptation In Organizations. *Organization Science, 5*(1), 98-118.

Volkoff, O., Strong, D.M., and Elmes, M.B. (2007). Technological Embeddedness and Organizational Change. *Organization Science, 18*(5), 832-848.

Yamauchi, Y., and Swanson, E.B. (2010). Local assimilation of an enterprise system: Situated learning by means of familiarity pockets. *Information and Organization, 20*(3-4), 187-206.

Zhu, K. and K. L. Kraemer. (2005). Post-Adoption Variations in Usage and Value of E-Business by Organizations: Cross-Country Evidence from the Retail Industry. *Information Systems Research, 16*(1), 61-84.

Generative Control Theory for Information Systems

Benoit Raymond
Computer Information Systems Department
J. Mack Robinson College of Business
Georgia State University
Atlanta, Georgia USA

Dr. Richard Baskerville
Computer Information Systems Department
J. Mack Robinson College of Business
Georgia State University
Atlanta, Georgia USA

Abstract

Increasing information security losses, coupled with more closely regulated security risk disclosure, are raising the importance of information security standards in designing information security. Despite the growing importance and variety of these standards and the fact that their adoption requires a large investment, there is a lack of theoretical development in this area. This paper develops a better understanding of information security standards by analyzing their controls. This analysis led to the discovery of a new class of controls, generative controls, previously unrecognized in the IS literature and the proposition of a new theory for information systems, generative control theory. This theory explains how the presence of generative controls allow the standardization of information security controls across widely different kinds of organizations while, at the same time, enabling their own adaptation to various organizational settings with underlying concepts such as generative controls, deferred controls definition, adaptive security, and surface and deep compliance. The theory, illustrated by the comparison of two prominent information security standards, ISO 27002:2005 and PCI, is useful for

understanding how standards may differ in the nature, structure and coverage of their controls depending on their goals. This comparison shows how the ISO standard, not just in terms of sheer size, but in other fundamental ways requires more elaborate design for both its implementation and audit and is also more vulnerable to creative compliance issues. In return, however, organizations attain more flexibility and better security alignment.

Keywords: generative control theory, information system, information security, information security standards, generative controls, deferred control definition, adaptive security, surface compliance, deep compliance

Introduction

Constant and emerging information security threats, such as malware and hacker attacks, have become a prominent aspect of the environment of management information systems (MIS). Because of these threats, security and control of MIS is now a fundamental necessity in order to guarantee that organizational information is available, reliable, and private. The struggle between threats and security controls continuously escalates. Hackers work continuously to improve attack tools, techniques and methods to find new ways to break down databases, networks and computers. In response, MIS professionals continuously strive to gain and hold technological superiority over the attackers, and to mitigate information security threats. As no organization is excluded for these threats, more and more companies are spending an ever increasing amount on information security. In the Computer Security Institute's 2008 survey of 522 US firms, most were spending more than 2% of their IT budget on security (Richardson, 2008). Despite this investment, the average 2009 loss due to computer security incidents was US $234,244. Sixty-four percent of firms incurred losses because of malware infections, one-third were phishing

victims, nearly 30% had losses due to denial of service, and one in five had losses due to computer-based financial fraud. These fraud losses averaged nearly a half-million per victim (Peters, 2009).

Given this obvious growth in computer security risk, we could expect regulators to increasingly require public disclosures of MIS security and control vulnerabilities to shareholders in public company. Such risk disclosures must be highly visible in order to properly assess share values. New regulation is not really required. Public risk disclosure laws were enacted in the early 2000s the wake of a series of worldwide corporate financial collapses, such as Enron and WorldCom. These regulations require disclosure of many kinds of risk that include those arising from information security. More than 28 countries passed such legislation (Neil, 2005). Examples include expansions of the European Union 8th Directive (Braiotta, 2005), the Canadian National Instrument 52-109 (CSA/ACVM, 2008), the Australian Corporate Law Economic Reform Program (CLERP 9), (Grey & Dale, 2005; Robins, 2006) and the U.S. Sarbanes-Oxley Act (AICPA, 2010). While this collection of legislation varies in depth, the laws still have many similar features (Braiotta, 2005; Grey & Dale, 2005; Neil, 2005; Robins, 2006) and most of them have more or less shifted oversight responsibility and power from the professions into the hands of government regulators. The impact on disclosure of information security risks has been sharp and dramatic. In a study of more than 20,000 SEC reports, the percentage of firms reporting information about security activities doubled in the years immediately after the enactment of Sarbanes-Oxley legislation (Gordon, Loeb, Lucyshyn, & Sohail, 2006).

In order to comply with these regulations, control gaps must be disclosed. Such gaps are most easily identified by comparing the organizational control practices with one of the widely accepted standards. This common practice among auditors, relying on external standards to benchmark compliance, is illustrated by the use of broad quality management standards such as ISO 9001 (Liebesman, 2007). For the purpose of identifying and disclosing gaps in information security control, auditors may start with standards such as ISO/IEC 27002 (Haworth & Pietron, 2006) or the COBIT framework (Braganza & Hackney, 2008). As a result, the legislation drives organizations seeking to avoid information security risks (and thereby ethically avoiding such risk disclosures) into compliance with a security standard. Compliance with an acceptable security standard is likely to satisfy auditors that there are no substantial risks arising from information security and control gaps. The operational effect of these information security disclosure requirements is an immediate institutionalization of information security standards. Moreover, if not required by law or mandated by business partners, organizations have nonetheless strong incentives to adopt standards to protect the security of their information.

Overall, the institutionalization of these information security standards and legislations has had a dramatic effect on the way information security controls are specified and evaluated which, in turn, has strong implications for both practitioners and researchers. Regarding practitioners, as the number and variety of information security standards continues to increase; organizations are forced to make critical decisions regarding which ones to adopt. Furthermore, despite their good intentions, information security standards have been proved difficult and expensive to implement properly (Braganza & Hackney, 2008). Regarding researchers, it is worth noting that since controls included in information security standards have often emerged from practical experience

rather than research, theory regarding information security standards usually takes a *post hoc* descriptive role. We can summarize the present situation (above) as follows. Driven by the impact of compliance, information security standards are growing in importance and variety. Large amount of resources are being dedicated to their adoption. The stakes are high; because the security risks organizations seek to control are commonplace and costly. Finally, there is a lack of theoretical development in the security standards area.

The objective of this paper is to develop a better understanding of these information security standards (which lie at the heart of information security control) and to contribute to theory in a contemporary era in which historical security lapses have harmed society. More specifically, this paper aims at providing novel insights to these research questions:

1) How can information security controls be standardized across widely different kinds of organizations?
2) How can information security standards be classified and compared?

To help answer these research questions, we developed a taxonomy for classifying controls in standards and analyzed the structure and content of several information security standards. The results of this analysis motivated the proposition of a new theory called "generative control theory for information systems (GCT)", that demonstrates how information security standards assure appropriate and effective security by enabling their own adaptation to different organizational settings with varying information security needs. This theory explains how information security standards can differ in fundamental ways and why these differences have been instilled in the standards in order to achieve different goals. Moreover, the theory suggests insights into how different organizations, through adaptive mechanisms, can be standardized, and

yet be distinctive. Importantly, it also shows how organizations can abuse standards by creatively complying with these adaptive mechanisms.

This paper is structured as follows. First, we present an overview of information security standards. Second, we describe the different steps involved in the controls analysis of information security standards. Third, we define the generative control theory that we propose in this paper as well as its underlying concepts. Fourth, we distinguish generative control theory by comparing it with the concept of business rules. Fifth, generative control theory is applied to compare two information security standards. Sixth, we present the results of this comparison and interpret them. Finally, this paper concludes with a summary of its contributions.

Overview of Information Security Standards

Information security standards have emerged from several bodies and evolved with multiple purposes that also led to many forms. This standards landscape continues to grow and evolve as new standards and revisions continue to be launched. While not exhaustive, Table 1 lists examples of information security standards categorized by the scope of their standards-setting bodies. For example, standards can be developed by international organizations, national governments, professional organizations (as standards of professional practice) or by industry groups.

Table 1. Examples of information security standards.	
Categories of standard-setting bodies	Examples
International Standards	ISO/IEC 15408 ISO/IEC 27002:2005 or 17799:2005 ISO/IEC 27001:2005 OECD Guidelines RFC 2196
Government Standards	ACS133 BS 7799 German IT Baseline Protection Manual US NIST 800 Series
Professional Standards	CobIT (Control Objectives for Information and related Technology) ITIL (Information Technology Infrastructure Library)
Industry Standards	PCI (Payment Card Industry)

Perhaps the most prominent information security standard is the ISO/IEC 27002:2005 (confusingly, ISO renumbered its standard 17799:2005 as ISO/IEC standard 27002:2005 in 2007). It is a highly detailed and comprehensive code of practice in the area of information security management intended to be useful to a large population of organizational forms and sizes. Its prominence attracts references to it from other standards. For example, CobIT provides a mapping document to illustrate how the two standards can be integrated effectively (IT Governance Institute, 2006). The development of the ISO/IEC 27002:2005 standard has also provided insights into how stakeholder interests can shape such international standards (Backhouse, Hsu, & Silva, 2006).

Analyzing Standardized Controls

In order to analyze the structure and content of information security standards, our approach adopted the principle that all science begins first by the study of diversity in order to distinguish

one population of objects from all of the other objects that exist in the universe, followed second by the study of uniformities within each population. This is why our approach first started with "systematics", a term McKelvey (p. 13) adopted from biology to describe the search for diversity. Systematics is a form of scientific inquiry that logically divides phenomena into populations that functional science can then examine to reveal generally shared characteristics. Systematics has three concerns: (1) classification, which involves the construction of an organization of formally designated classes, and the identification and assignment of phenomena to each class; (2) evolution, which involves the study of the emergence, decline and genealogy of these classes, and (3) taxonomy, which involves development of theories and methods for classification (Mckelvey, 1982). Then, our approach involved "functional science", a term McKelvey (1982) defined as the search for uniformity or the discovery of universal laws governing the behavior, function, and processes of population of objects.

Classification of Standardized Controls

Classification schemes develop from a central concern for the intended purpose and audience of the scheme. A control classification scheme can be helpful in discovering controls, analyzing and validating them, and even designing for them (von Halle, 2002). In our case, we wanted our classification scheme to be able to distinguish behaviorally-based controls from other forms of information security controls. The presence of this type of controls is of high interest to both practitioners and researchers as humans are assumed to be less predictable than computers. However, most current inventories of controls follow an activity-based organization and thus do not support such a classification task.

Formal inductive classification schemes involve gathering a sample of the objects to be classified and studying the shared characteristics. Groups of shared characteristics provide potential criteria for classification purposes. The quality of the formal classification is measured by three standards: parallelism, mutual exclusivity, and completeness. The classification is parallel when the same criterion has been used to define each object's class. Where the classification is hierarchical, the criterion must be the same at each level of the hierarchy, but it may be different at different levels. The classification is mutually exclusive when each class is independent of all others. No object should satisfy differing classes. Where the classification is hierarchical, objects may fall into multiple classes at different levels, but should not fall into multiple classes at the same level. Finally, the classification is complete when all objects fit into some class within the classification scheme (Goldstein, 1978; Sandman, Klompus, & Yarrison, 1985). A variation of the formal inductive classification approach involves partitioning. Partitioning implies dividing an object into its different parts and is necessary when an object is constructed from several constituent objects, as each of which may fall into different classes. Attempts to classify such compound objects can be flawed because they will satisfy a classification criterion for multiple classes (Goldstein, 1978; Sandman, et al., 1985).

Our approach for developing a classification scheme combined deductive and inductive classification approaches. Under this approach, we first developed a modified version of an existing controls classification system: the Baskerville's (1988) nine control classes classification scheme that operates along two dimensions (see Table 2). The first modification involved the addition of a new class of controls, "behaviorally-based controls". Most particularly, there was clearly a singular characteristic of behaviorally-based controls that enabled us to categorize these

controls separately from other types of controls. That characteristic was its embodiment in human behavior. Put simply, behaviorally-based controls are "things that people do". An example would be engaging in security awareness training. We then attempted to deductively classify a sample of controls from the ISO 27002:2005 standard. We particularly studied the overlaps: controls that fell into multiple categories. This first step enabled us to determine difficulties with distinguishing a particular class for a control. Indeed, we found that most controls from the sample fell into multiple classes under this classification system, which violates the principle of mutual exclusivity. Moreover, it is worth noting that because the original Baskerville nine-class classification system (1988) uses multiple criteria, it violates the principle of parallelism. Overall, this deductive exercise provided the experience necessary to begin a formal inductive classification process.

Table 2. Baskerville's Nine Control Classes (1988)			
Locus	Avoidance	Tolerance	Mitigation
Physical			
Logical			
Communications			

To distinguish behaviorally-based controls from controls that are inherently provided by computers, we decided to start with our new class of behaviorally-based controls as our first class of controls and continue to improve our classification scheme. A second modification involved the creation of a second class of controls: information technology (IT)-based controls, or "things that IT artifacts do". An example would be encryption processing. A third modification involved the creation of a third class of controls that resided in more intimate material objects that are not IT-related: physical controls. This category, perhaps less happily, might be characterized as "things that stuff does". An example would be walls around a computer room. But because it becomes difficult to distinguish IT artifacts from other physical

objects (that is, computers are stuff), we looked for a more definitive criterion. For this purpose, we chose the concept of *raison d'etre,* a term we use as meaning the purpose that justifies the existence of a specific control. For example, while an automobile may offer several functionalities, its *raison* is transportation. Looking across our classification system, we can now distinguish behaviorally-based controls by their *raison* because the chief purpose of these controls is to influence human behavior. Similarly we can now distinguish IT-based controls by their *raison*, which is data or information. Lastly we can now distinguish our third class of controls, physical controls, by their *raison*, which is material. Our selection of this final value for our criterion now enables us to distinguish IT-based controls as primarily defined by their delivery of data or information from physical controls as primarily defined by their delivery of material barriers, etc.

The use of the concept of *raison d'etre* as a criterion operates with some elegance. For example, it eliminates the confusion between a computer system as a physical object and a computer system as a purposeful data processing object. It is a fact that a computer may print out information on paper, and paper is a material object. But the *raison* of the computer system is the information carried on the paper medium. In this way, IT artifacts are clearly classified in a separate category from physical objects. This also applies to IT-based controls and physical controls.

Moreover, experience with our deductive-inductive classification process demonstrated the existence of a fourth class of controls. This class of controls usually involves high level generic controls such as requirements for policies mandating controls. These are controls that are

actually involved in initiating, creating, precipitating or generating more specific controls. An example is a control requiring the organization to have policies about security. The *raison* of these controls, their defining purpose, is the production of more specific controls which, in this example, may translate into further requirements for locks, encryption, or firewalls. This fourth class of controls is referred to as the generative control class. The controls included in this class are distinguished by the *raison* criterion of generating further controls.

We use the term generative in the metaphorical sense usually (but erroneously) attributed to Chomskian linguistics (Truex & Baskerville, 1998). Generative controls would align with the popular concept of "deep structures" that generate the "surface structures" of a system. In common usage, the term "deep structure" is often used to represent a common ground, the foundation from which other related structures, such as "surface structures", are derived. For example, the universal grammar can be considered as the "deep structure" from which sentences, or "surface structures", are derived. In our case, deep structures are represented by *generative* controls, more generic in nature, that create surface structures represented by *surface* controls, more specific in nature, embodied in policies, standards or laws and relating to human behavior, physical objects, and IT artifacts. That is, *surface* controls represent the controls belonging to the behavioral, IT-based and physical control classes. Since generic *generative* controls generate more specific *surface* controls, it is important to note that the generative control class proposed in this research operates at a different level of abstraction than the three other control classes. As discussed later in this paper, this difference in the level of abstraction between control classes has important implications for the adaptability and audit of standards. Table 3 summarizes the criteria for classifying controls.

Table 3. Criteria for classifying controls	
Control Classes	*Raison*
Physical	Elements whose *raison* is material, in forms subject to the laws of nature, characterized or produced by the forces and operations of physics
IT-based	Elements that are primarily IT-based artifacts whose *raison* is data or information
Behavioral	Elements that are the processes of people whose *raison* is decision and/or human conduct
Generative	Elements whose *raison* is initiating, creating, precipitating or generating more specific forms of controls

As mentioned earlier, in order to avoid the problem of controls falling into multiple classes under this classification system, thus violating the principle of mutual exclusivity, partitioning may be necessary to properly classify the controls contained in any common compendium. Indeed, different kinds of controls may be conflated into a single descriptive text. As partitioning involves dividing an object into its parts, it requires to parse the different components from the description of the various controls. For example, consider the following description of a control policy drawn from the ISO 27002:2005 information security standard:

12.4.3 Access control to program source code

Control: *"Access to program source code should be restricted"*

Such a general description lumps together several different kinds of controls, or at least permits several interpretations of suitable controls. Therefore, this general control must be partitioned into its component parts before it can be classified. Based on the text provided in the standard to help explain the nature of this control, it is possible to partition this meta-level control into the following component parts:

- Generative control class: "Procedures should be established for the management of program source code and program source libraries".

- Behavioral control class: “The issuing of program sources to programmers should be authorized”.
- IT-based control class: “An audit log should be maintained of all accesses to program source libraries”.
- Physical control class: “Program listings should be held in a secure environment”.

Defining Generative Control Theory (GCT)

Interestingly, although the presence of a distinctive class of controls, the generative control class, makes a lot of sense, it is not well recognized in the IS literature. Compared to *surface* controls which are of the physical, IT-based, or behavioral type, that are more specific and precise in nature and thus are given with a higher degree of exactness, these *generative* controls are more generic and imprecise in nature. Surface controls. Acknowledging the presence of generative controls in standards is important as it has strong implications for both researchers and practitioners because generative controls permit the standards setters to defer the exact definition and implementation of standardized controls to people present in the situation being secured. As such, compared to the specification of surface controls, the presence of generative controls in control standards represents a deeply different approach to specifying controls, one that is anchored to an entirely different theoretical perspective. As they involve a distinctly different set of assumptions than surface controls, they respond to a different set of logical concepts. Together, these elements make us believe that the presence of these generative controls in standards constitutes a different *theory* of control, one with at least five interrelated concepts that are not present in standards defining only surface controls. This set of concepts constitutes the

basis for a new theory for information systems that we propose in this paper: Generative Control Theory (GCT). We now describe the five interrelated concepts underlying GCT.

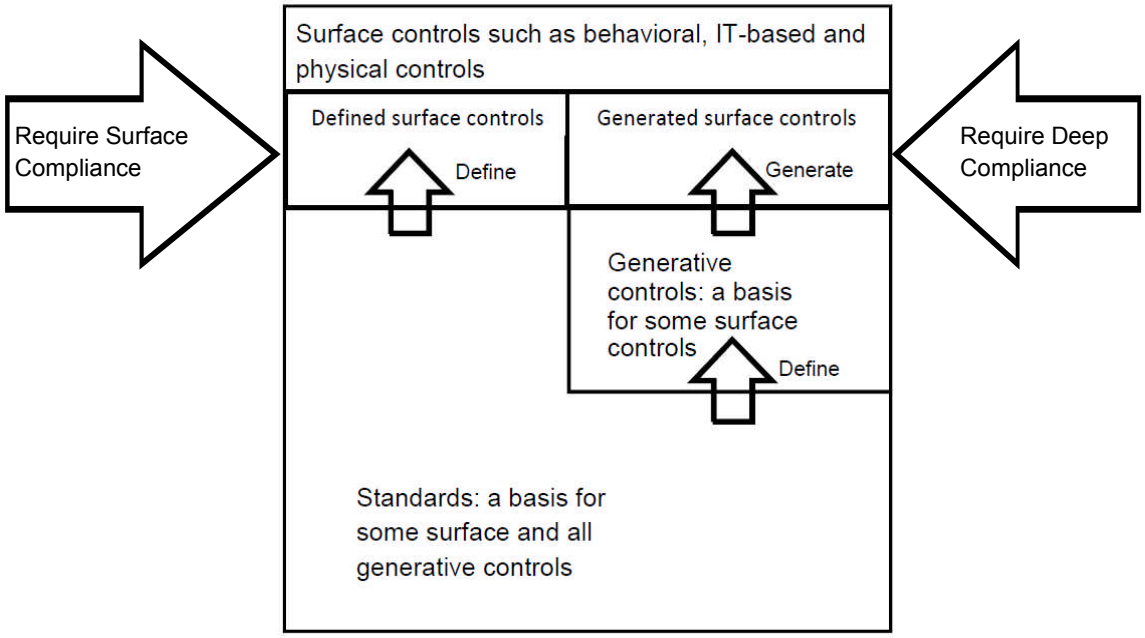

Figure 1. Sources of surface controls and their impact on compliance requirements

Figure 1 shows the impacts of the presence of generative controls in standards. Standards may define surface controls only or a combination of surface and generative controls. In standards defining generative controls, these latter will serve as the basis for generating other surface controls, and as a result, some surface controls will be directly defined by the standard while some other surface controls will be generated by the generative controls defined by the same standard. As mentioned earlier, surface controls, which may be of the physical, IT-based, or behavioral type, are more specific and precise in nature. Surface controls directly defined by a standard usually enjoy a high degree of exactness as they are not resulting from an interpretation process. Because people implementing the standard within the organization do not have to interpret these controls, they only require surface compliance. In contrast, surface controls generated by generative controls defined in a standard do not enjoy this same degree of exactness as they are the result of the interpretation of generative controls that are more generic and

imprecise in nature. Because people implementing the standard within the organization have to rely on their own interpretation of generative controls, these surface controls require deep compliance. In other words, when their precision is directly defined in a standard, surface controls only require surface compliance. In contrast, when their precision is the result of the interpretation of imprecise generative controls, surface controls require deep compliance.

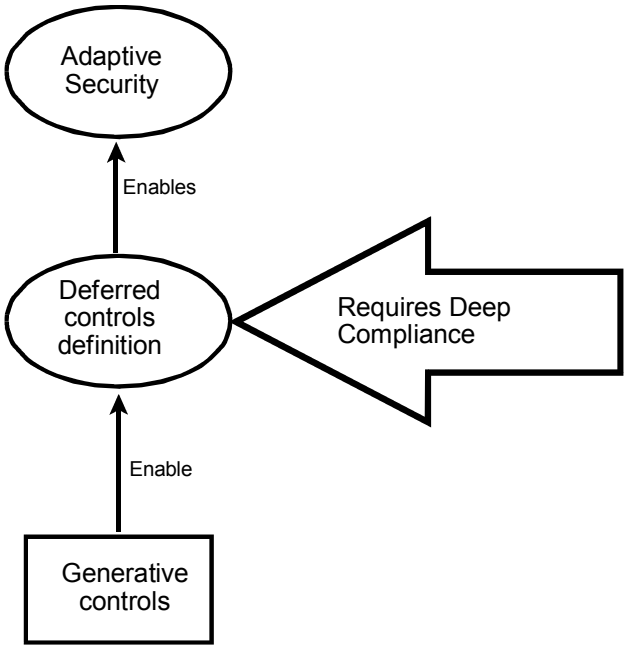

Figure 2. Impacts of the presence of generative controls in standards

Generative Controls

Generative controls are high level, generic and imprecise controls such as requirements for policies mandating controls. The *raison* of these controls, their defining purpose, is to initiate, create, precipitate or generate more specific controls such further requirements for locks, encryption, or firewalls. They represent the deep structures that create surface structures represented by *surface* controls, more specific in nature, embodied in policies, standards or laws and relating to human behavior, physical objects, and IT artifacts. By being high level, generic and imprecise in nature, generative controls enable the concept of deferred controls definition

(see Figure 2) which is an effective way to ensure the appropriateness and effectiveness of controls included in the standard to various organizational security settings.

Deferred Controls Definition

The concept of deferred controls definition means that rather than defining surface controls in precise terms, only the requirements for such surface controls are specified in the standard. The precise definition and design of surface controls are deferred to authorities "on the ground" with detailed knowledge of the organizational security setting. By embedding the concept of deferred control definition, generative controls defer the formulation of the work of the standards-setting bodies to the end implementers of the standards. Indeed, generative controls operate at a "meta" level by defining what the surface controls must accomplish, their objectives, while allowing the adopting organization to determine exactly how the control should operate and what form or design it should take. The concept of deferred control definition, by providing some flexibility to the adopting organization, enables adaptive security to standards (see Figure 2).

Adaptive Security

The concept of adaptive security refers to the fact that the standard enables some flexibility to adopting organizations by allowing them to respond, in some ways, to the standard in their own fashion. As standards are generally adopted by different types of organizations, the concept of adaptive security is motivated by the requirement for information security controls that are appropriate for the organizational security setting in which they are implemented. It assumes that organizational security needs are unique to a certain degree, and that no universal security plan will provide the ideal security protection for all types of organizational forms and instances.

Because it becomes impossible to define appropriate information security controls for each organizational security setting, information security standards must allow some form of adaptive security in order to be applicable and relevant to a large number of organizations of different forms and sizes. This requires control designs to be generated at the time an information system is developed, deployed, and/or secured in preparation for its operation in a specific organizational setting.

Controls that are defined precisely in control standards, such as surface controls, may be well suited and more readily implementable by some adopting organizations but they can also become irrelevant more easily for other organizational settings. Just as developers of software packages, standards setters need to position their products on a continuum consisting of generality (or applicability) on one hand and specificity (or usefulness) on the other hand. The concept of adaptive security seeks to allow standards to be applicable to a large number of organizations while permitting their mandated controls to be relevant and effective to each adopting organization. In control standards, adaptive security is achieved by the use of deferred controls definition embedded in generative controls (see Figure 2) that allows the exact form of security controls to be tailored to the security needs of the organization adopting the standard. Given that the standards-setting bodies determine which controls are to be generative, and which are not, the proportion of generative controls is likely vary between standards as well as their organizational adaptability.

Moreover, because many organizations are themselves adaptive in response to continuous change in their environment, structure, culture, etc., their organizational security needs and

settings are also likely to change over time. Such organizations need processes for routine controls regeneration such that controls are redesigned as needed to match changes in their organizational security needs. In control standards, adaptive security is achieved by the use of deferred controls definition embedded in generative controls (see Figure 2) that provides the ability for implemented information security controls to evolve and adapt without necessarily misaligning the organization with security control standards. In turn, this flexibility or adaptability provided by the use of deferred controls definition embedded in the standard requires deep compliance (see Figure 2).

Surface Compliance

The concept of surface compliance means that the compliance of control is evaluated by comparing the actual implementation of the control with its precise definition or specification in the standard. Surface compliance is only available when precise control definition is done by an external standard or policy. Since the control definition is not deferred to authorities on the ground, this ensures that interpretation of a control's definition is minimized. Therefore, surface compliance is only applicable to surface controls directly and precisely defined in standards (see Figure 1). Under surface compliance, only one type of evaluation is required: the actual implementation of the control as compared to what is required by the external standard or policy.

Deep Compliance

In contrast, deep compliance refers to a situation in which the external standard or policy defers the precise definition of a control through the use of generative controls (see Figure 2). This is the case of surface controls generated from generative controls defined in a standard (see Figure

1). Deep compliance is required because these surface controls are the result of the interpretation of generative controls that are more generic and imprecise in nature, by people implementing the standard within the organization. Under deep compliance, two evaluations are required: (1) the actual design of the surface control as compared to its requirement in the standard and (2) the actual implementation of the surface control as compared to the results of its generated design. Therefore, not only the actual implementation of the surface control needs to be evaluated but also, and most importantly, its design. Indeed, the sound implementation of a control may only offer limited information security protection if its design is flawed.

It is important to note that achieving surface compliance can be perfectly adequate for an organization adopting a standard that contains only non-generative controls. What is more of a concern is when only surface compliance is achieved by an organization adopting a standard or policy containing generative controls. To illustrate the difference between surface and deep compliance and for simplicity and clarity reasons, the same control, 12.4.3 Access control to program source code, drawn from the ISO 27002:2005 standard seen earlier in this document will be used once again as an example. As mentioned earlier, to achieve surface compliance means that the exact implementation of the non-generative controls, that is, the controls belonging to the behavioral, IT-based, and physical control classes, follows what is precisely defined in the external standard or policy. By partitioning this example of a meta-level control into its component parts as seen earlier, we can see that it is easier for an organization's management and their auditors to evaluate the surface compliance of surface controls defined directly and precisely in the standard by looking, for instance, at the presence of physical or digital signatures and keys, passwords, and audit logs. In contrast, evaluating deep compliance

for surface controls generated from imprecise generative controls included in a standard is less straightforward and requires the evaluation of the soundness of both the design and implementation of the procedures established for the management of program source code and program source libraries. For an organization adopting such meta-level controls, achieving surface compliance would be necessary but not sufficient as the actual design of the procedures established needs also to be evaluated based on its requirement in the standard. Indeed, while procedures may have been established and implemented, their flawed design may not address critical risks related to the management of program source code and program source libraries.

Distinguishing GCT

This section is about comparing and distinguishing generative control theory, that is, how it is similar to and different from other related concepts. Basically, this whole idea of so called generative controls is not really a new one as other authors just used other terms to refer to this type of meta-level controls. Indeed, concepts such as policies and guidelines are closely related, and statements such as business rules can certainly be established with a broad scope at a high level of expression. However, what is interesting is the fact that the presence of this type of controls in information security standards is not well recognized yet in the IS literature.

GCT and Business Rules

To better distinguish GCT, a comparison between the concepts of generative controls and business rules can be helpful as they offer many similarities but also important differences. In order to do that, we need first to define the concept of business rule. This is not as straightforward as it may seem as no industry standard definition exists for the term business

rule, or even for rule, and that consequently there is also no universal business rule classification scheme (von Halle, 2002). We adopt the definition of business rule proposed by The Business Rules Group (2001) as a statement that defines or constrains some aspect of the business. This must be a term or fact (structural assertion), a constraint (action assertion), or a derivation. It is intended to assert business structure or to control or influence the behavior of the business by constraining and/or supporting it. Informally speaking, business rules are the guidelines, rules and mandatory policies governing interactions among employees, customers, suppliers, and automated systems and through which business leaders steer or guide the business in its activities (von Halle, 2002). As such, they serve as the guidance system that influences the collective behavior of an organization's people and information systems so that the organization behaves and evolves as its leaders intend. The intentions of an organization's business leaders and the needs of the business constitute the desired logic of the business (Morgan, 2002).

Similarities between GCT and Business Rules

First, both generative controls and business rules are acting as requirements or specification of a process or procedure without being a description of it. Indeed, while business rules represent a set of statements defining the constraints and conditions that can act as a specification for a process, controlling the behavior of a business or system in various ways in diverse situations, they do not represent a description of a process or procedure (Morgan, 2002). Just like generative controls only stipulate the requirements for a process, business rules do not impose the exact mechanisms through which this process operates. A business rule should define "what" should be the case and should not prescribe "who" invokes the rule, "when" the rule is executed, "where" the rule executes, and "how" the rule is to be implemented (defined in design) (Morgan,

2002). Moreover, just like generative controls included in a standard, there should be one cohesive body of rules that should apply and be enforced consistently *across* processes and procedures for all relevant areas of business activity (Business Rules Group, 2003).

Second, both surface control statements derived from generative controls and business rules can be established with varying levels of structure. All levels have a structure but occupy different points along the trade-off between accessibility of business meaning and desirable automation properties (Morgan, 2002). Choosing the appropriate level of structure to use when establishing business rules or when derivating surface control statements from generative controls is a decision that should be made carefully. On one hand, the establishment of more formal and structured statements is likely to make them easier to automate and assess (Morgan, 2002). On the other hand, he states that most people at the business level would be far happier with more colloquial, informal and less structured statements.

Third, generative controls as well the surface controls derived from them, and business rules may address similar concerns. For example, generative controls included in information security standards are mainly concerned with reducing information security risks to the organization or minimizing their impact. This is in accordance with (Morgan, 2002) who states that while precise business rules are commonly associated with various aspects of the business, they can be classified under one or more general concerns, such as reducing risks to the business or minimizing their impact, making the most efficient use of corporate resources or controlling or managing the flow of work.

Fourth, the effectiveness of generative controls, the surface controls derived from them, and business rules is highly dependent on the accuracy of their interpretation. Just as the logic underlying a business needs to be translated or specified into a series of more precise business rules to be effective, generative controls included in a standard need also to be translated into a series of surface controls, more precise in nature. This is what we refer to as the translation process. Because many downstream decisions will depend on what these more precise statements say, it is worth spending some up-front effort on making sure that they are accurately stated and properly aligned to the aims of the business (Morgan, 2002). Indeed, just as a word can have different meanings depending on the context of use, the fact that different interpretations of the same generative control included in a standard can occur makes this translation process a very important one.

Differences between GCT and Business Rules

Although the concepts of generative controls, including the surface controls derived from, and business rules share many characteristics, some important differences exist that need to be taken into account. First, an important difference exists concerning their scope. Business rules are established for a specific organization. They are basic to what the business knows about itself, that is, to basic business knowledge (Business Rules Group, 2003). They represent the desired logic of this organization, its specific needs and intentions from its business leaders (Morgan, 2002). Two organizations may have a similar size and operate in the same industry and market, but it is unlikely that they will have the same internal logic. On the contrary, generative controls included in a standard are, by nature, established to be applicable to a large number of organizations of various sizes and operating in different industries and markets. The number of

organizations will vary according to the scope of the standard and its standard-setting body. The standard can apply to organizations operating in a specific industry or not, national or international organizations, governmental, public or private-owned organizations, etc.

Second, a difference generally exists regarding their level of abstraction. Business rules and surface controls generated from generative controls are more precise in nature and thus operate at a lower level of abstraction. Generative controls, in contrast, are imprecise by nature and thus operate at a higher level of abstraction. While generative controls may need to be partitioned first in order to derive surface controls statements, business rules are "atomic" in that they cannot be broken down or decomposed further into more detailed business rules (Morgan, 2002). If reduced any further, there would be loss of important information about the business.

Third, generative controls and business rules differ regarding their defining body. Business rules are established by an organization's past or current business leaders. It is their responsibility to determine the difference between a successful and unsuccessful business event (Morgan, 2002). They establish business rules that define all possible and permissible conditions for a successful business event along with those that are not permissible. Therefore, a business event is unsuccessful when it fails to meet the business's rules for a successful business event. As such, business rules represent the set of conditions that govern a business event so that it occurs in a way that is acceptable to the business (Morgan, 2002). In contrast, generative controls included in a standard are usually established by a standard-setting body comprised of various partners with different backgrounds.

The differences between generative controls, surface controls and business rules have important consequences. The first one is the fact that generative controls included in a standard are much more difficult to implement and audit than surface controls or business rules. Business rules are determined by the organization's business leaders and while they can change over time, they constitute an ultimate and precise source of reference for assessing the design, implementation and use of business rules within the organization. As such, the organization's business leaders, as domain experts, can be of great help in reducing possible misinterpretations of established business rules. For example, they can easily explain the specific logic or meaning underlying these business rules, their specific intentions, and the specific needs of the business. All these elements make it easier to create a fact model ensuring that the business rules established are appropriate and coherent between each other.

In contrast, generative controls included in standards generally lack this precise and easily accessible source of reference for assessing the design, implementation and use of surface controls derived from them within adopting organizations. First, the people who created these generative controls in the standard, likely a standard-setting body comprised of various partners, are usually not easily accessible to explain the precise meaning or logic underlying these generative controls. Moreover, even if they were accessible, they are not domain experts for each organizational setting for which the standard is adopted. Therefore, the standard itself act as the main source of reference. Second, while many standards offer some implementation guidance and additional information, the fact that a standard is intended, by nature, to be applicable to a large number of organizations, makes it difficult for them to mandate specific controls or provide precise guidance on how to design and implement surface controls for each organizational

setting. To illustrate this argument and for simplicity and clarity reasons, the same control drawn from the ISO 27002:2005 standard seen earlier will be used once again as an example:

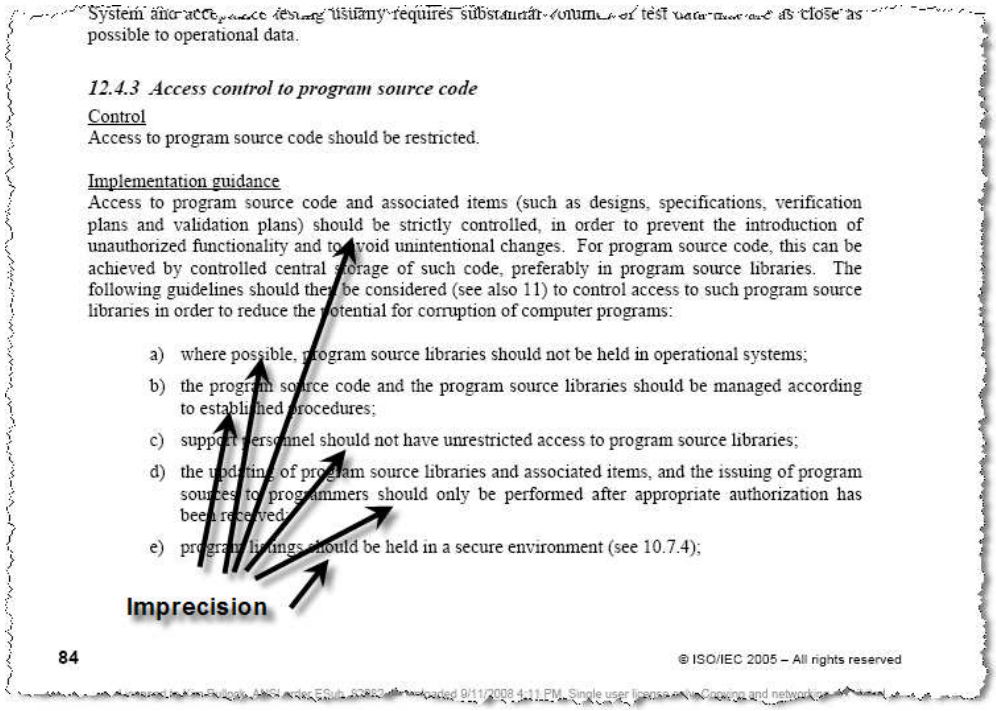

Figure 3. Example of a control in ISO 27002:2005

Although this additional information provides some guidance for designing and implementing surface controls generated from generative controls included in the standard, it does not describe the exact mechanisms through which the surface controls will operate. Moreover, the use of terms such as “can”, “may” or equivalent in a standard simply say that something might or might not be the case or that the rule could be optional, which is too vague to be useful (Morgan, 2002). People within organizations adopting the standard are therefore forced to rely on their own judgment and interpretation about the best way to capture the logic embedded in the generative control to design and implement further surface controls that will meet the organization’s specific needs. However, it is worth noting that what may appear as a weakness of standards, it is in fact something intended upfront. Indeed, providing more precise guidance would defeat one important objective of any standard: to be applicable or adaptable to a large number of widely

different kinds of organizations. Despite these good intentions, the interpretation of generative controls and their translation into surface controls, leading ultimately to one or more implementations of the generative control, is a human activity, with consequent opportunities for the introduction of errors and creative compliance issues (Morgan, 2002).

GCT and Creative Compliance

To generate sound surface controls from generative controls included in information security standards, a good understanding of both the logic underlying these generative controls and the organization's information security setting is required. This is often not an easy task as generative controls included in standards are general in nature and, as with any statement, can be vague or even incomplete (Shah, 1996). Creative compliance issues arise from the fact that different interpretations of the same generative control included in a standard can occur and thus create a variety of results both in terms of control design and implementation in response to this generative control. Indeed, the presence of imprecise generative controls in standards gives adopting organizations the opportunity to design their own controls and implement them in different ways. While this flexibility potentially offers the benefit of more relevant and appropriate controls, taking into account the specificities of the organizational security setting at hand, it can also be abused by allowing the organization to easily misrepresent its compliance. In one comparative case study, organizations typically force-fit existing safeguards into compliance requirements in order to minimize actual changes to systems. While the representations were questionable in the study, the reporting was sufficiently convincing for the auditors to accept that these local adaptations were adequate (Braganza & Hackney, 2008). The issue illustrates why the implementation and audit of controls derived from generative controls is more difficult.

Indeed, evaluating the soundness of their design and implementation requires a deep understanding of both the standard itself and the organizational security setting at hand. As the soundness of control designs and implementations needs to be evaluated for deep compliance, these creative compliance issues have strong implications for both the organization's management and their auditors. Indeed, a misunderstanding of the generative control's logic is unlikely to produce appropriate surface controls that reduce risks to the organization or minimize their impact. Moreover, of high significance is the fact that regulates may also develop schemes which fulfill the letter of the rules, but undermine their spirit (Shah, 1996). Indeed, although the implementation of inappropriate surface controls that do not achieve these goals is certainly an unfortunate result, a worse case is the implementation of surface controls that, in fact, increase the risks to the organization or their impact.

Therefore, while the use of generative controls in standards provides the benefit of adaptive security, likely to result in more appropriate and effective controls for adopting organizations, their presence in standards also results in an additional burden to (1) adopting organizations by requiring them to design controls based on high-level requirements in standards, and (2) their auditors by requiring them to evaluate the exact design and implementation of the surface controls generated from these generated controls. For example, the lack of uniformity in the framework for testing or probing compliance to the "shall" requirements of ISO 9001 creates a serious problem for companies which seek registration to ISO 9001 since there is a large gap between the ISO 9001 clauses and their interpretation for the field of software (Walker, 1998). So much that, according to him, this creates considerable problems for those who create and

maintain software quality management systems against the ISO 9001 standard — and those who interpret those requirements for compliance purposes (quality systems auditors).

Applying GCT: Comparing Standards and their Organizational Adaptability

To illustrate the usefulness of GCT, we decided to use it as a framework for comparing and contrasting information security standards. Some of them are positioned at a high level as they mostly focus on the specification of control objectives, and only provide few specifications for surface information security controls beyond managerial processes. These high level standards centralize management processes that tailor security controls to the adopting organization. Two major examples of such high level standards are CobIT and ISO/IEC 27001.

We first analyzed the structure of CobIT and ISO/IEC 27001:2005, and found an overwhelmingly large proportion of generative controls with only a few surface controls belonging to the other and more precise controls classes. Based on these results, we then decided to concentrate on two lower level and more detailed information security standards: ISO/IEC 27002:2005 and PCI data security standards. These two standards were chosen for two main reasons. First, both information security standards are widely recognized and used. A study (Baskerville, 2005) showed that surveyed companies following ISO 27002 represented the largest percentage (41%). Second, although they both represent lower level and more detailed information security standards, they have widely different foci as ISO/IEC 27002:2005 represents an overall security management framework while PCI's main focus is to prevent credit card information theft. Therefore, the analysis of the structure and content of these two information security standards should provide us with interesting insights regarding the

distribution of their control classes as well as the content and coverage of their information security controls. These two information security standards are now presented in further detail.

ISO 27002:2005 provides a security management framework, and detailed recommendations for security policies along with a wide variety of controls such as access controls, communications controls, physical security controls, personnel security controls, etc. This standard was developed from the original British Standard, BS 7799, and with the endorsement of the International Standards Organization, has substantial adherents. It contains 11 security control clauses, one being an introductory clause introducing risk assessment and treatment. Each of the 10 other clauses contains a number of main security categories representing a collective total of 39 main security categories. Each of them contains a control objective stating what is to be achieved and one or more controls that can be applied to achieve the control objective. The description of each of these controls is composed of three parts: 1) a specific control statement to satisfy the control objective, 2) implementation guidance which provides more detailed information to support the implementation of the control and meet the control objective and 3) further information that may need to be considered, for example legal considerations and references to other standards. Overall, the ISO/IEC 27002:2005 standard includes a total of 133 controls.

The Payment Card Industry (PCI) data security standard was established by the PCI Security Standards Council. It contains 12 data security standard requirements related to the payment card industry. These standard requirements are organized in 6 logically related groups, which are control objectives. Worth noting, the PCI data security standard requirements only apply to an organization if a Primary Account Number (PAN) is stored, processed, or transmitted in processing payment card transactions. These security requirements apply to all system

components, which are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances while server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external Internet applications.

Data Analysis Methods and Results

In this research, the unit of analysis was the 133 information security control statements included in the ISO 27002:2005 standard and the 64 controls found in the PCI data security standard. Together, they represented the primary data of this study. These information security controls were evaluated based on two main aspects: their structure, as represented by the classes of controls they are belonging to, and their coverage.

Controls Structure Analysis

The controls structure analysis was composed of several steps. In the first step, a spreadsheet was created to list and organize the various controls and control classes. In the second step, the spreadsheet was used as a template for the classification process by two independent coders. Each control was coded into one or more control classes based on the nature of the control and

the information supporting the control provided in the standard. Since many of these controls are general in nature, they often needed, as shown previously, to be first partitioned into its component parts before being classified. The result was that a large number of these controls were considered as belonging to more than one control class. This explains the existence of several overlaps for the two standards as the total number of all the controls in the four control classes exceeds the total number of controls included in each standard. Regarding intercoder reliability measures, the coding process of ISO 27002:2005 resulted in an overall percentage of agreement of 70% and a Cohen's kappa value of 0.32 while results were respectively 73% and 0.49 for the PCI data security standard. These Cohen's kappa values represent satisfactory agreement under conditions of four coding categories. Such higher numbers of categories increase the potential disagreement and lowers the expected kappa accordingly (Sim & Wright, 2005).

In the third step, the coding results from the two independent coders were compared and the discrepancies were classified in two categories: "hard" discrepancies and "soft" discrepancies. The need for creating two types of discrepancies resulted from the fact that, as each control could be coded into any possible combination of one to four different control classes, a total of twenty-four coding combinations was possible thus reducing the chances to get identical results for the two independent coders. Soft discrepancies represented controls for which at least one control class was common to the two independent coders while hard discrepancies represented controls for which no control class was common. For controls involving soft discrepancies, we used the common control classes as the point of agreement and thus these control classes were the only ones considered for further analysis. By doing so, we reduced the possibility of disagreement and

randomness. For controls involving hard discrepancies, a fourth step involving a qualitative approach was performed. This fourth step consisted of a meeting with the two independent coders and an information security expert during which all the hard discrepancies were analyzed, discussed, and finally resolved, thus resulting in 100% agreement. The classification into control classes resulting from this meeting was considered as the final classification of these controls and thus these control classes were the only ones considered for further data analysis. In the fifth step, the spreadsheet was used to calculate statistics about the distribution of controls into control classes for the two standards.

The results of the controls structure analysis are presented in Table 4 which compares the distribution of controls between the different control classes for the two standards. As mentioned earlier, the total number and the total percentage of all the controls in the four control classes exceeds the total number and percentage of controls included in each standard because of the existence of several overlaps for the two standards. For each row representing a specific combination of control classes, the number of controls belonging to this specific combination, as well as its corresponding percentage based on the total number of controls in the standard, are indicated. For example, for the specific combination of control classes represented by the Generative control class, the number 43 in the second column means that 43 controls out of 133 belong to this control class, this number representing 32% of the 133 controls included in the ISO 27002:2005 standard. The same description also applies to the third column representing the distribution of the 64 controls included in the PCI data security standard.

Table 4. Distribution of controls for ISO 27002:2005 and PCI		
Control classes	ISO 27002:2005 (133 controls)	PCI (64 controls)
Generative controls	43 (32%)	16 (25%)
Behavioral controls	56 (42%)	23 (36%)
IT-based controls	46 (35%)	30 (47%)
Physical controls	12 (9%)	4 (6%)
Generative AND Behavioral controls	10 (8%)	2 (3%)
Generative AND IT-based controls	1 (1%)	0 (0%)
Generative AND Physical controls	0 (0%)	0 (0%)
Generative AND Behavioral AND IT-based controls	0 (0%)	0 (0%)
Generative AND Behavioral AND Physical controls	1 (1%)	0 (0%)
Generative AND IT-based AND Physical controls	0 (0%)	0 (0%)
Behavioral AND IT-based controls	6 (5%)	4 (6%)
Behavioral AND IT-based AND Physical controls	1 (1%)	1 (2%)
Behavioral AND Physical controls	2 (2%)	1 (2%)
IT-based AND Physical controls	1 (1%)	0 (0%)

Based on a Venn diagram, Figure 4 below shows the mapping of all the 133 controls included in the ISO 27002:2005 standard.

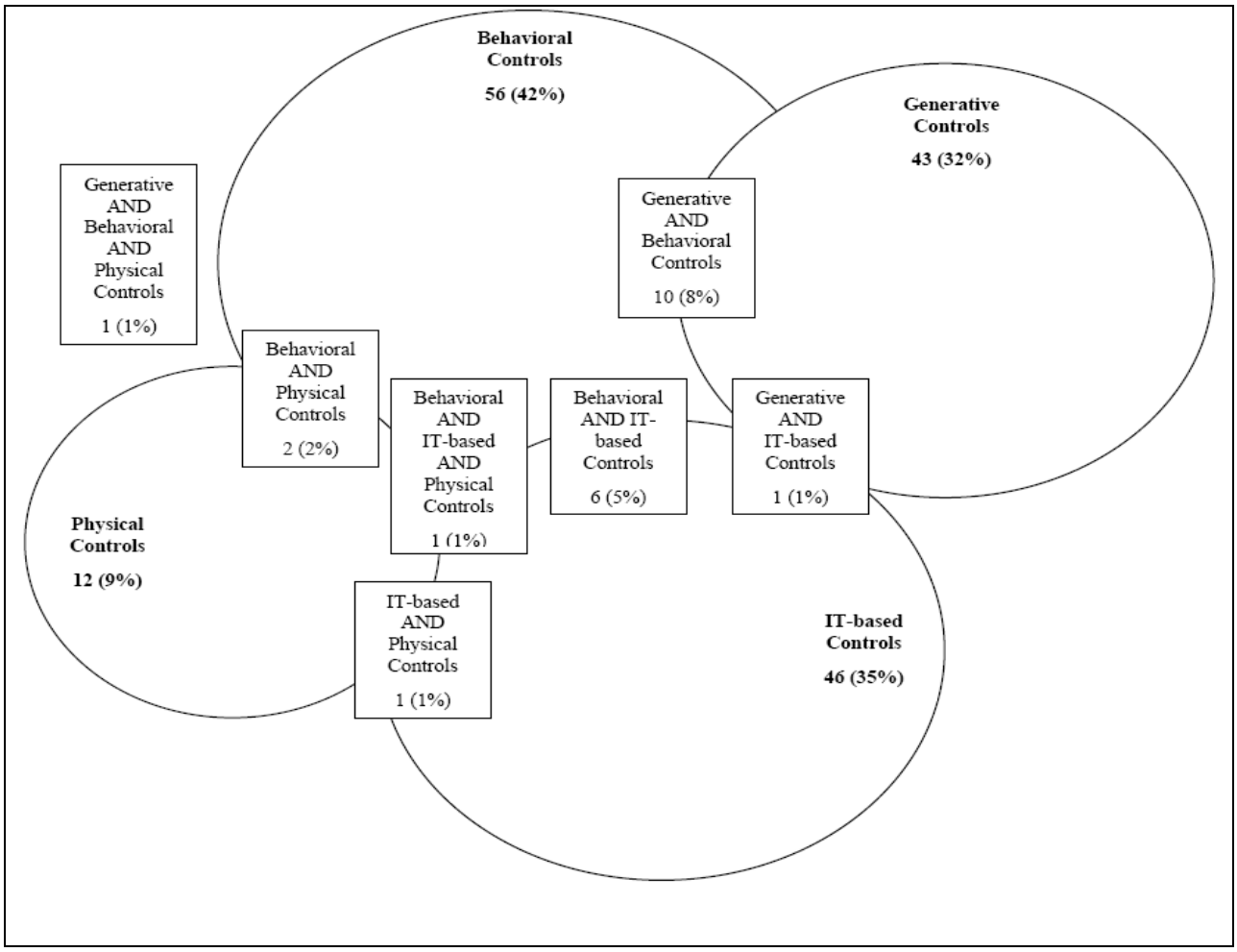

Figure 4. Mapping of the 133 controls included in the ISO 27002:2005 standard

In Figure 4, each "circle" represents a control class with the size of each circle increasing according to the total number of controls belonging to this specific control class. The amount of overlap between circles varies according to the number of controls that are belonging to multiple control classes, a higher number being represented by a larger amount of overlap between circles thus meaning a closer relationship between these control classes. For example, 10 controls are belonging to both Generative and Behavioral control classes. From Figure 4, we can see by the size of the circles that Behavioral controls represent the main control class with 56 out of 133 controls (42%) belonging to this class. The next biggest circle is the one representing IT-based controls, followed closely by the one representing Generative controls. We can also observe that

the biggest amount of overlap between circles is between the Generative and Behavioral control classes, meaning that the relationship between these two control classes is the strongest. The next biggest amount of overlap between circles is between the Behavioral and IT-based control classes. On the other hand, representing only one control, are the relationship between the Generative and IT-based control classes and the relationship between the Physical and IT-based control classes. These represent the weakest relationships as we can see by the amount of the overlap between circles. Following the same pattern, Figure 5 is based on a Venn diagram representing the mapping of the 64 controls included in the PCI data security standard.

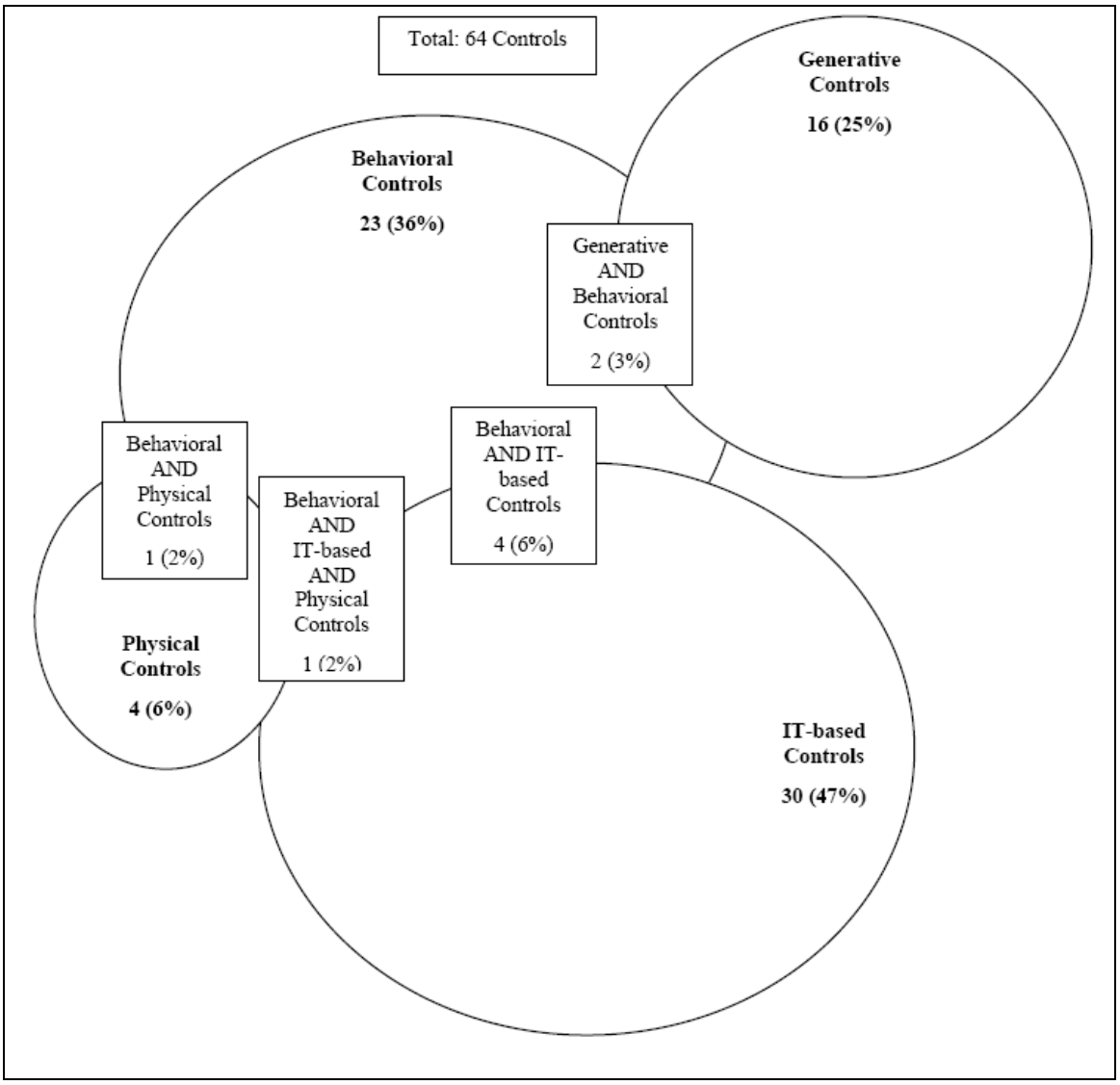

Figure 5. Mapping of the 64 controls included in the PCI data security standard

From Figure 5, we can see by the size of the circles that IT-based controls represent the main control class with 30 out of 64 controls (47%) belonging to this control class. The next biggest circle is the one representing Behavioral controls, followed in third by the one representing Generative controls. We can also observe that the biggest amount of overlap between circles is between the Behavioral and IT-based control classes, meaning that the relationship between these two control classes is the strongest. The next biggest amount of overlap between circles is between the Generative and Behavioral control classes. On the other hand, representing only one

control, is the relationship between the Behavioral and Physical control classes. This represents the weakest relationship as we can see by the amount of overlap between these two circles. Other similar interpretations can be easily made the same way by looking at Figure 5.

Controls Coverage Analysis

For this analysis, a table was first created to list all the 133 controls in the ISO 27002:2005 according to their original classification in terms of security control clauses, security categories, and controls objectives. Then, when possible, each control was matched with one or several of the 64 controls included in the PCI data security standard. This analysis permitted to identify which aspects of information security were covered by both standards and which were not. The results from this analysis demonstrated that while both ISO 27002:2005 and PCI, two information security standards with differing foci and scope, contain information security aspects that are not specifically covered in the other standard, controls related to security aspects that they both cover are not conflicting with each other and therefore they may in fact well complement each other.

Interpreting the Results Using GCT

As mentioned earlier, GCT is useful for recognizing and understanding the degree of organizational adaptability of a standard. The results of the controls analysis performed in this study offer several important and interesting insights regarding information security standards. First, these two information security standards incorporate a substantial body of Generative Controls. Forty-three out of 133 controls (32%) of the ISO 27002:2005 standard and 16 out of 64 controls (25%) in the PCI data security standard are generative controls. While this type of

controls has been somewhat neglected in the IS literature, this result confirms not only the existence but also the importance of generative controls and the need for the creation of a new class for controls involved in initiating, creating, precipitating or generating surface controls. According to GCT, the substantial presence of generative controls in these two standards means that they are motivated by the need for adaptive security, and operationalize deferred control definition. Indeed, the exact nature of the generated surface controls being implemented under these standards will be determined by designers closer to the moment of implementation. As a result, these controls may be uniquely fitted to the organization's security needs. It also means that the actual design of the generated controls can be changed without necessarily misaligning the organization with the standard. Furthermore, this result means that these two standards require deep compliance in many areas, which in turn means that auditors must not only determine whether the controls are in place and well implemented, but whether the design of the controls has been appropriately generated according to both the standard and the organizational security setting.

Second, the fact that the ISO standard has a larger proportion of generative controls (32%) than the PCI standard (25%) means that it has a greater degree of organizational adaptability. This is coherent with the purpose of this standard which, as a code of practice for information security management, provides guidelines and general principles intended to be useful to a large population of organizational forms and sizes. As such, the standard is offered as a starting point for developing surface information security controls. The language of the standard acknowledges that some recommended controls may not be suitable to every organization, and that additional controls, not covered by the standard, may be necessary in some organizations.

The larger proportion of generative controls also means that the ISO standard requires a higher degree of deep compliance than the PCI standard. Because the ISO standard is deeper, it involves more elaborate implementation work because many controls require both controls generation (an appropriate design) and implementation when applying the standard. The ISO standard also requires more elaborate auditing, because both the generation and implementation of 32% of the controls must be audited. Obviously, the simple fact that the ISO standard is larger in terms of the total number of controls it includes means that the implementation and audit work resulting from the adoption of the ISO standard is substantially more involved than a PCI application and audit. The usefulness of GCT in explaining how organizations respond to security standards arises in this case from simple metrics indicating the more elaborate design and audit work required for ISO compliance than for PCI compliance.

Third, assumptions that different information security standards could not be usefully compared have been debunked by this study, in which effective comparisons of two widely recognized but different standards were provided. Fourth, this study supports the fact that it could be worth it, and in some cases necessary, for organizations to adopt multiple information security standards. This is especially true when these information security standards have differing foci and scope. Indeed, our analysis demonstrated that while both ISO 27002:2005 and PCI, two information security standards with differing foci and scope, contain information security aspects that are not specifically covered in the other standard, the controls related to security aspects that they both cover are not conflicting with each other and therefore they may in fact well complement each other. According to GCT, the substantial presence of generative controls in these two standards

means that they both operationalize deferred control definition. This adaptive mechanism, by allowing the exact nature of the generated surface controls being implemented under these standards to be determined by designers closer to the moment of implementation, help to reduce control conflicts between adopted standards.

Fifth, an important theoretical contribution of this research to the information security literature is the proposition of GCT along with its underlying concepts such as adaptive security, deferred control definition, generative controls, and surface and deep compliance. Together, they provide the reasons for, and the effects of the presence of generative controls in information security standards. Sixth, the development and application of GCT in this study permitted to reveal important issues, such as the risk for creative compliance, that were somewhat overlooked in the IS literature. Moreover, there are several other observations that emerge from this study that may be worth noting. These include a recognition of the fairly small role of physical controls in these two standards (9% for ISO, and 6% for PCI), and the tendency in the ISO standard to use a greater proportion of behavioral controls (42%) in contrast to PCI, which tends to use a greater proportion of IT-based controls (47%). Finally, while this study focused on information security standards, GCT and the insights it offers can also be applied to other standards as well.

There are insights to help avoid or mitigate undesirable issues related to standards. An emphasis on clarity is crucial for defining the surface controls generated from generative controls included in standards. Indeed, the most difficult problem is to make the logic underlying the controls understandable (Morgan, 2002). Partitioning a complex generative control into its different components will result in a set of small, more manageable units that are easier to understand,

design and implement. The surface control statements should be concise, unambiguous, consistent and compatible with each other (Morgan, 2002). He adds that the use of words such as "can", "may" or unqualified terms should be avoided as they are too vague to be useful and can make the control look optional. For standards' auditors assessing whether a specific control is necessary, and its design and implementation are aligned with the standard's intentions, they should investigate whether the meaning and business objective underlying the control are well defined, unambiguous, and appropriate, the control fully address associated risks, there are more efficient and effective ways of achieving the business objective (Morgan, 2002).

Finally, this research, as with any research, has a number of limitations. A first limitation is the fact that results from the coding and classification processes of controls included in the ISO 27002:2005 and the PCI data security standards necessarily represent a subjective interpretation of those controls. Future research is needed to establish more objective classifications, e.g., through survey research approaches. A second limitation is the fact that these results are based on the analysis of only two information security standards. Future research is needed to expand the analysis to include other information security standards. Since both the ISO 27002:2005 and the PCI data security standards have been observed as composed of a large proportion of behavioral and generative controls, it would be important to compare it with other information security standards to see whether the research finding holds in other cases. Another interesting analysis could compare the results from this study with the ones obtained from an analysis of the ISO 17799:2000, or BS7799 (Part 1) standards. As these two standards predated the ISO 27002:2005 standard, it might be interesting to see whether any trends related to information security control classes can be observed over time. Such studies could suggest if standards are

growing more, or less, generative or behavioral. Furthermore, as the concept of adaptive security has only received a theoretical treatment in this study, future research can look at whether the design of information security controls implemented in organizations change over time in response to evolving organizational security settings while continuing to be aligned with information security standards. Finally, our current figures do not show the presence of any feedback loop as we wanted to limit the scope of this research. As process theory would suggest that the establishment of standards can be seen as an iterative process, future research can look at how standards-setting bodies and organizations are interacting to produce appropriate information security.

Conclusion

Given the rising importance and variety of information security standards, the large amount of resources involved in their adoption, and the lack of theoretical development in this area, the objective of this paper was to develop a better understanding of information security standards and to introduce a new theory regarding the composition of such standards. By means of a controls classification taxonomy that we developed, two prominent information security standards were analyzed in terms of the content, structure and coverage of their information security controls. The results of this analysis not only helped to explain how standards can differ in fundamental ways and why the differences have been instilled in the standards in order to achieve different goals but it also contributed to the proposition of a new theory for information systems, "generative control theory (GCT)" useful for both researchers and practitioners . GCT highlighted the existence of a class of controls previously unrecognized in the IS literature, generative controls, and a set of underlying and interrelated concepts not present in surface

controls: adaptive security, deferred control definition, generative controls, surface compliance and deep compliance. It also explained how the presence of generative controls in standards can act as an adaptive mechanism helping to provide adaptive security by deferring their exact implementation to people present in the situation being secured. As such, generative controls allow the standardization of information security controls across widely different kinds of organizations, while, at the same time, enabling their own adaptation to various organizational settings. Moreover, GCT demonstrated how the proportion of generative controls in a standard influence its degree of organizational adaptability, why more elaborate work is required in implementing and auditing generative controls and how organizations can abuse standards by creatively complying with these controls. Finally, as the insights from this theory may also be useful to the study of other types of standards, we provided suggestions for generating surface controls from generative controls included in standards, the standard compliance auditing process, and for improving the establishment of controls in standards.

References

AICPA. (2010). Summary of The Provisions of the Sarbanes-Oxley Act of 2002 Retrieved 16 Feb, 2010, from http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/Summary+of+the+Provisions+of+the+Sarbanes-Oxley+Act+of+2002.htm

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly, 30*(SI), 413-438.

Baskerville, R. (2005). Best Practices in IT Risk Management: Buying safeguards, designing security architecture, or managing information risk? *Cutter Benchmark Review, 5*(12), 5-12.

Braganza, A., & Hackney, R. (2008). Diffusing Management Information for Legal Compliance: The Role of the IS Organization Within the Sarbanes-Oxley Act. *Journal of Organizational and End User Computing, 20*(2), 1-24.

Braiotta, L. (2005). An overview of the EU 8th Directive: the European Union prepares to issue its response to corporate malfeasance. *Internal Auditor*(April).

Business Rules Group. (2001). Defining Business Rules: What Are They Really? Retrieved January 18, 2010, 2010, from http://www.businessrulesgroup.org/first_paper/br01ae.htm

Business Rules Group. (2003). Business Rules Manifesto. Retrieved January 18, 2010, 2010, from http://www.businessrulesgroup.org/first_paper/br01ae.htm

CSA/ACVM. (2008). *Notice of National Instrument 52-109 Certification of Disclosure in Issuers' Annual and Interim Filings*. Ontario: Canadian Securities Administrators / Autorités canadiennes en valeurs mobilières.

Goldstein, M. (1978). *How We Know: An Exploration of the Scientific Process*. New York: Plenum.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy, 25*(5), 503-530.

Grey, K., & Dale, L. (2005). Australian companies and Sarbanes-Oxley: Governance regulation in a parallel universe. *Keeping Good Companies*(June).

Haworth, D. A., & Pietron, L. R. (2006). Sarbanes-Oxley: Achieving compliance by starting with ISO 17799. *Information Systems Management, 23*(1), 73-87.

IT Governance Institute. (2006). CobiT Mapping: Mapping of ISO/IEC 17799-2005 with CobiT 4.0 (Vol. 2007, Available from http://www.isaca.org/

Liebesman, S. (2007). ASQ Team Says QMS and EMS Standards Support SOX. *Quality Progress, 40*(10), 34-39.

Mckelvey, B. (1982). *Organizational Systematics: Taxonomy, Evolution, Classification.* Berkeley, Calif.: University of California Press.

Morgan, T. (2002). *Business Rules and Information Systems: Aligning IT with Business Goals*. Boston, MA: Addison-Wesley.

Neil, B. (2005). Global debate over controls. *The Internal Auditor, 62*(3), 50-54.

Peters, S. (2009). *2009 CSI Computer Crime and Security Survey Executive Summary*. New York: Computer Security Institute.

Richardson, R. (2008). 2008 CSI Computer Crime and Security Survey. Retrieved 1 Dec, 2008, from http://www.gocsi.com/

Robins, F. (2006). Corporate Governance after Sarbanes-Oxley: an Australian perspective. *Corporate Governance, 6*(1), 34.

Sandman, P., Klompus, C., & Yarrison, B. (1985). Scientific and Technical Writing, *Scientific and Technical Writing*. Ft. Worth, Texas: Holt, Rhinehart and Winston.

Shah, A. K. (1996). Creative Compliance in Financial Reporting. Accounting, Organizations and Society, 21(1), 23-39.

Sim, J., & Wright, C. C. (2005). The Kappa Statistic in Reliability Studies: Use, Interpretation, and Sample Size Requirements. Physical Therapy, 85(3), 257-268.

Truex, D., & Baskerville, R. (1998). Deep Structure or Emergence Theory: Contrasting Theoretical Foundations for Information Systems Development. Information Systems Journal, 8(2), 99-118.

von Halle, B. (2002). Business Rules Applied: Building Better Systems Using the Business Rules Approach. New York: John Wiley & Sons, Inc.

Walker, A. J. (1998). Improving the quality of ISO 9001 audits in the field of software. Information and Software Technology, 40, 865-869.

Conclusion

Consistent with its overall research objective, this dissertation contributed to knowledge and theory about the influence of IT on organizations and their members. Composed of three separate but related studies, each study adopted a unique research perspective and examined different aspects of the relationship between IT and organizations. Therefore, in addition to this main objective, this dissertation provided novel insights on various aspects of the relationship between IT and organizations.

The first study, broadest in scope, provided a fifty-year overview of the dominant theoretical perspectives that IS researchers have used to study the influence of technology on organizations and their members. Without being exhaustive, it identified, for each decade, the dominant theoretical perspectives used in the IS field. These theoretical perspectives were illustrated by the selection and description of two exemplars published in the decade and their implications for researchers and practitioners were explained. The results of this study showed that in each of the last five decades, a new dominant theoretical perspective was developed and adopted to extend the previous decade's rhetoric by getting even further away from technological determinism in the sixties and closer to more balanced causal arguments explaining the consequences of IT on organizations and their members. This study suggested also important implications for future research such as the need for IS researchers to study and theorize the materiality of IT artifacts and potential approaches that IS researchers can used for restoring theoretical attention to material IT artifacts in IS research. However, IS researchers must not reproduce history by rediscovering determinism; rather this study advocates a balance between material and human

agencies in their explanation of causal arguments of IT outcomes on organizations and their members.

The second study provided insights about the theoretical aspects of the relationship between IT and organizations. Looking more specifically at how IT artifacts influence the design and performance of organizational routines, it proposed three key extensions to organizational routines theory supported by the development of new concepts and models. First, it proposed to consider artifacts in general as latent material agents, possessing a potential to exert material agency that exist independently but is only materialized through their human enactments. This study also highlighted the distinctive characteristics of IT artifacts which, in turn, help them to become embedded in organizational routines. Second, this study proposed a process model explaining how material agency of IT artifacts can alter the repertoire of technology's enactments and thus contribute to the production of varying and indeterminate routine performances that are characteristics of generative systems. Third, this study proposed a new model describing the various elements and relationships involved in organizational routines. This new model acknowledges that IT artifacts can become embedded in organizational routines. As an integral part of organizational routines, IT artifacts can influence the design and performance of organizational routines by playing mediating and generative roles in the recursive relationship between the ostensive and performative aspects of these organizational routines.

The third and last study can be considered as the application of concepts presented in the second paper of this dissertation to the study of information security standards. Information security standards and their information security controls may be considered as IT artifacts embedded in

organizational routines, thus representing an integral part of these routines. Just as written with procedures, information security standards may incorporate elements of the ostensive aspect of the organizational routine and play roles similar to those that can be played by the ostensive aspect of the routine. For instance, information security controls included in information security standards can play guiding, accounting and referring roles. Information security standards can also incorporate elements of the performative aspect of the organizational routine. The establishment of specific information security controls can be seen as the result of past human actions in which information security was compromised or at risk for the organization. The incorporation of elements of the ostensive and performative aspects of the organizational routine in information security standards gives them a material aspect since these elements are no longer only traces in the mind of actors.

When embedded in organizational routines, information security standards can influence the design and performance of organizational routines by playing two types of overarching roles. First, information security standards embedded in the organizational routine can play a *mediating role* in the recursive relationship between the ostensive and performative aspects of the organizational routine. This mediating role arises from the fact that, as argued earlier, they can play roles that are similar to those played by the ostensive and performative aspects of the organizational routine. Furthermore, as argued earlier, when organizational elements are incorporated in IT artifacts such as information security standards, they acquire a material aspect that interacts with and affects their ostensive and performative aspects (Volkoff et al. 2007).

Second, information security standards embedded in the organizational routine may play a *generative role* in the recursive relationship between the ostensive and performative aspects of the organizational routine. Information security standards can act as what Giddens (1984) calls *allocative resources*. Mastering the content of these information security standards may grant more knowledgeable users, such as standard compliance experts, a valuable power to perform organizational routines in novel ways. Moreover, as demonstrated earlier, a substantial part of the information security controls included in information security standards are generative controls. Their purpose is to generate more precise controls (surface controls) by specifying only their requirement and general objective. The generation of surface controls based on generative controls is left to people inside the organization adopting the standard and is largely based on their interpretation and judgment about these generative controls. Because the broad definition of generative controls can be interpreted in different ways, the specific design and implementation of surface controls are likely to be different across organizations adopting the same information security standard. This introduces variations, or new performances, regarding the implementation of the standard. As such, information security standards can be seen as contributing to the production of varying and indeterminate performances (generation of surface controls) that are characteristics of generative systems. The role of standard compliance auditors can be seen as the legitimating process of novel standard's implementations or performances as they need to evaluate their adequacy based on the standard itself and the local information security setting. Only changes perceived as legitimate will eventually lead to enduring changes to the ostensive aspect of the organizational routine. Together, these arguments support the treatment of information security standards and their controls as IT artifacts that can become embedded in organizational routines, thus representing an integral part of these routines.

In addition, the third study contributed to a better understanding of the design and composition of information security standards by looking at the structure, content and coverage of information security controls included of two prominent information security standards: ISO 27002:2005 and PCI data security standards. It also helped to explain how standards can differ in fundamental ways and why the differences have been instilled in the standards in order to achieve different goals. This study involved the development of a controls classification taxonomy that eventually led to the proposition of a new theory called generative control theory (GCT) and a set of underlying and interrelated concepts: adaptive security, deferred control definition, generative controls, surface compliance and deep compliance. This theory and its underlying concepts explain how the presence of a large number of generative controls in standards acts as an adaptive mechanism helping to provide adaptive security by deferring their exact design and implementation to people present in the situation being secured. GCT also explains how the proportion of generative controls in a standard influences its degree of organizational adaptability, why more elaborate work is required in implementing and auditing this type of controls and how organizations can abuse standards by creatively complying with these generative controls. Finally, this study provided suggestions for generating surface controls from generative controls included in standards, auditing an organization's compliance with standards, and for improving the definition of controls in standards.

Research Limitations and Directions for Future Research

As with any research, this dissertation has a number of limitations and can be extended in several ways. In this section, I present some of these limitations and propose directions for future

research to address them and explore new avenues. Regarding the first study, we recognize that the identification of dominant theoretical research perspectives used in research on IT influence on organizations and their members as well as exemplars to illustrate them is a subjective activity. Moreover, mapping them to specific time periods is not a straightforward exercise as it also involves subjectivity since IT research streams often overlap decades. Therefore, other researchers may come up with different results and conclusions. This research can be extended by the review of additional IS journals and by looking at other aspects of the relationship between IT and organizations.

Regarding the second study, an obvious limitation is that the proposed models, concepts and supporting arguments have not been empirically tested. This could be done in future research. This will not only help to validate the three extensions to organizational routines theory that are proposed but also to better understand the dynamics involved in IT post-adoption behavior. Researchers could also investigate how different types of IT artifacts, possessing different characteristics and thus offering different opportunities and constraints for human action, influence the design and performance of organizational routines. For instance, compared to custom-made information systems, IS packages offer many differences in terms of design, functionality, and work processes. Moreover, since IS packages incorporate standard work processes, they can be seen as more rigid and constraining than custom-made information systems for organizations implementing them. As such, it would be interesting to see whether the specific characteristics of IS packages have an impact on how this type of IT artifact influences the design and performance of organizational routines. Volkoff et al. (2007) state that organizational change can result from the generation of second-order effects resulting from the

interactions between organizational elements that are embedded in technology and those that are not. Future research can investigate whether our extension of organizational routines theory to include embedded IT artifacts provides an adequate mechanism to explain these second-order effects.

Regarding the third study, we recognize that the codification and classification of information security controls included in standards are essentially subjective activities. Future research is needed to establish more objective classifications of information security controls, e.g. through survey research approaches. Another limitation is that the study's results are based on the analysis of only two information security standards. Researchers are invited to expand the analysis of information security standards by studying additional ones. For instance, since both the ISO 27002:2005 and the PCI data security standards have been found to be composed of a large proportion of behavioral and generative controls, it would be important to verify if the research findings still hold for other information security standards. Another interesting analysis can assess whether any trends related to information security controls found in information security standards can be observed over time. For instance, it would be interesting to determine whether information security standards are growing more, or less, generative or behavioral. As such, the results from the third study can be compared with the ones obtained from an analysis of the ISO 17799:2000 or BS7799 (Part 1) standards as these two standards predated the ISO 27002:2005 standard. Furthermore, as the concept of adaptive security has only received a theoretical treatment in this study, future research can look at whether the design of information security controls implemented in organizations change over time in response to evolving organizational security settings while continuing to be aligned with information security

standards. Finally, to limit the scope of this study, the figures do not currently show the presence of any feedback loop. Since process theory would suggest that the establishment of standards can be seen as an iterative process, future research can investigate how standard-setting bodies and organizations are interacting to produce appropriate information security.

This dissertation represents a small step only toward a better understanding of the influence of IT on organizations and the individuals. Future research can extend this work by adopting other research perspectives and examining other aspects of the relationship between IT and organizations.

References

Chen, Irene Y. L. (2007). The factors influencing members' continuance intentions in professional virtual communities – a longitudinal study. *Journal of Information Science, 33*(4), 451–467.

Giddens, A. (1984). The Constitution of Society. University of California Press, Berkeley. 402 p.

Kallinikos, J. (2004). Deconstructing information packages: Organizational and behavioural implications of ERP systems. *Information Technology & People, 17*(1), 8-30.

Morris, D., Tasliyan, M. and Wood, G. (2003). The Social and Organizational Consequences of the Implementation of Electronic Data Interchange Systems: Reinforcing Existing Power Relations or a Contested Domain? *Organization Studies, 24*(4), 557–574.

Volkoff, O., Strong, D. M., & Elmes, M. B. (2007). Technological Embeddedness and Organizational Change. *Organization Science, 18*(5), 832–848.