AIS: Challenges to Technology Implementation

Pierangelo Rosati, Theo Lynn

Abstract

The convergence of cloud computing, mobile technology and big data technologies are transforming information technology faster than ever before. While there is an established knowledge base of known implementation issues relating to project management, technology, user resistance, organisation/environment and outsourcing, digital technologies introduce new challenges. This chapter summarises traditional challenges in information system implementation and discusses some of the issues arising from the deployment of digital technologies including migration to the cloud, security, data protection and ICT governance, contractual issues in the cloud, big data and mobility.

Introduction

Technologies to support the processing and distribution of data evolved over the last five decades from systems for mere data processing to systems designed to support decision making from a wide range of perspectives, whether at the organisation, group or individual level and the operational, tactical or strategic level. More recently, the emergence of digital technologies are challenging our assumptions around technology adoption. More powerful and intelligent infrastructure combined with unparalleled access to data is creating new business models that introduce new complexities; complexities that accounting information systems are not insulated from. Similarly, research on the adoption of information systems is not new and these are, for the most part, applicable to accounting information systems. Like other disciplines, accountants and financial professionals face emerging adoption challenges resulting from new technologies, not least external and internal compliance reporting (Belfo & Trigo, 2013).

This chapter starts with a discussion of the traditional challenges in information systems adoption. We examine the empirical literature from five perspectives i.e. project management, technology, user resistance, organisational/environmental and outsourcing challenges. One could argue that cloud computing, and in particular public cloud computing, is a natural extension of outsourcing in that firms not only outsource their information systems but their entire infrastructure on a shared distributed basis. The traditional accounting information systems market has been disrupted by cloud computing with legacy software vendors migrating to the cloud often merely to compete with native cloud accounting service providers, such as Xero. However, cloud computing both exacerbates traditional information systems challenges and creates new ones. The final section of this chapter discusses some of the emerging challenges for accounting information system adoption related to cloud computing, big data analytics and mobile technologies. This includes a discussion on challenges related to migration to the cloud, security, data protection and ICT governance, and contractual issues.

Traditional Challenges to Information Systems Implementation

There is a well-established literature base on the traditional challenges of information systems implementation providing evidence of the negative consequences for organisations both in terms of financial losses (Nelson, 2007; Laumer & Eckhardt, 2012; Maier et al., 2013) and litigation (Wailgum, 2009). In addition, commentators report IT project failure rates remain high. The Standish

Group (2020) reports that roughly two out of three IT projects typically fail, a relatively constant rate since 2011. Causal analysis of such implementation failures suggests that failure can be attributed to well-known issues in IT management studies which we label as *Traditional Challenges*, namely: *Project Management Challenges*, *Technology Challenges*, *User Resistance Challenges*, *Organisational/Environment Challenges*, and *Outsourcing Challenges*. These challenges should not be viewed as independent from each other. On the contrary, they are deeply interconnected and interdependent. All these potential issues should be evaluated but also the relationships between them.

Project Management Challenges

Information systems projects are particularly challenging from a management perspective mainly because of their hidden complexity and uncertainty (Peffers et al., 2003). Furthermore, information systems projects require the intense collaboration of several different groups of stakeholders, e.g. IT staff, users, and management (Dechow & Mouritsen, 2005; Quattrone & Hopper, 2005). Therefore, the ability to communicate and coordinate the activities of the group is extremely important (Ewusi-Mensah, 1997; Sumner, 1999).

Nelson (2007) shows that mistakes concerning processes or people account the majority of failures i.e. 45 percent and 43 percent respectively. The remaining 12 percent is due to product (8 percent) or technology mistakes (4 percent). This highlights the importance process and people management in information systems projects. Nelson (2007) analyses 99 projects conducted by 74 organisations over a seven-year period and comes to the conclusion that project failure is rooted in a series of missteps by project managers. Such mistakes (i.e. *Classic Mistakes*) can be grouped in four categories[1] - people, process, outputs and technology. From a people perspective, two key challenges emerge. Firstly, careful implementation of the team configuration is critical to ensure the team has all the individual capabilities required in the project, and members are able to create productive working relationships (Lakhanpal, 1993; Fui-Hoon Nah et al., 2001). Secondly, it is important to keep the team members motivated throughout the project since motivation is a well-known driver of productivity and quality (Borcherding et al., 1980; Boehm, 1981). Problems amongst team members typically arise, and in such cases, the project manager should deal with a problematic team member as soon as possible and, ideally, achieve a win-win solution. Conflicts may compromise group motivation or intra-group relationships resulting in project failures (Larson & LaFasto, 1989).

The second category of missteps in information systems projects is process issues. Smith & Reinertsen (1998) term the earliest stage of a project as the "fuzzy front end". The fuzzy end denotes all time and activity spent on an idea prior to the first official group meeting. Understanding the "fuzzy front end" has been a challenge for different types of organisations (Reid & De Brentani, 2004). Detailed and better understanding of the project requirements and the activities envisaged within a project may lead towards a successful implementation. Commentators suggest project management tend to waste time in this phase due to ineffective governance processes (Khurana & Rosenthal, 1997; Umble & Umble, 2001) thus resulting in an aggressive implementation schedule. Such overly optimistic schedules put excessive pressure on team members (McConnell, 2006). An acceptable trade-off in terms of time dedicated to project planning and implementation would increase the likelihood of project success. Finally, it is important to assess and control project risk (Aloini et al., 2007). Project managers may feel somewhat helpless managing risk particularly when risks are outside of their immediate control. However, risk management is critical (Cervone, 2006). Risk can be reduced (or eliminated) through problem remediation activities in the project plan, transferred to other activities or third parties (e.g. software vendor), absorbed by simply planning the required actions, or avoided by implementing quality controls. A honest risk assessment during the project planning phase will lead to more effective and efficient decision making throughout the project lifetime and has a clear impact on the project outcomes (Chapman & Ward, 2003).

[1] See McConnell (1996) for further details.

The third category concerns the output of the project (i.e. product). Often developers and project managers tend to add additional features, capabilities or changes which are expected to increase user satisfaction or systems effectiveness (Addison and Vallabh, 2002; Elliott, 2007; Malhotra et al., 2012). This so-called 'feature-creep' can lead to unnecessary costs, higher project complexity and delay (Landis et al., 1992; Murray, 2001). Therefore, it is important that project managers define clearly what the outputs and the boundaries of the project are.

The final category of missteps relates to technology. New technologies can be viewed as a panacea for problems. Nelson (2007) labels this tendency as the "silver-bullet syndrome". However, new technologies change constantly and are, therefore, unstable (Fraser et al., 2007). What seems the best solution today, might not be tomorrow and the search for silver bullets prevents deeper analyses into organisational needs and priorities (Lyytinen & Robey, 1999). As technology evolves, management may be tempted to switch tools in the middle of a project, which can be detrimental from a technological and motivational perspective.

Technology Challenges

Traditionally, information systems tend to present as large integrated, process-oriented packaged software designed to meet most needs of organisations (Pulakanam & Suraweera, 2010; Strong & Volkoff, 2010; Grabski et al., 2011). However, Markus (2000) points out that such systems address only 70 percent of the needs of the average organisation. Both providers and organisations have improved their ability to configure and implement enterprise systems over time, but a certain misfit between organisational needs and system characteristics still persists (Strong & Volkoff, 2010). Existing misfits create significant challenges in adopting such systems and in evaluating the success of the implementation. Strong & Volkoff (2010) classify possible misfits into six categories and identify, for each category, two types of misfits, namely deficiencies and impositions. A deficiency is a systems feature that the organisation needs but is missing in the system, while an imposition is a problem that the organisation has to face because of the system's inherent characteristics.

Functionality. In some instances, the usage of an information system may reduce process efficiency or effectiveness. Functionality deficiencies are due to the impossibility of performing simple tasks because of system restrictions (e.g. minimum amount required for a purchase order); these issues are usually fixed with little customisation or future releases. Functionality impositions arise when the system prevents users from performing tasks in a non-standard order. Information systems may not allow such actions because of the level of integration and standardisation of the business processes required by the system (Gattiker & Goodhue, 2005; Volkoff et al. 2005).

Data. Data misfits arise when data or data characteristics provided or needed by the system lead to data quality issues e.g. inaccuracy or inaccessibility. A data deficiency issue for example may emerge when the number of product attributes is not sufficient. In contrast, a data imposition issue may arise where a common data definition has not been implemented across the system.

Usability. A usability misfit occurs when the system requires more non-value added steps to complete a task. A common usability deficiency is inappropriate report designs. The difficulty in using data because of different identifiers (e.g. product code vs purchase order) is, instead, an example of usability imposition.

Role. Role misfit can be one of the most problematic. These occur when the end user roles in the information system are inconsistent with the roles that end users hold in the organisation. These may create workload imbalances and bottlenecks causing a significant loss in efficiency. A role deficiency occurs when a role in the organisation is diffused across many roles in the systems. A role imposition misfit, instead, arises when a role in the system has more responsibility than in the organisation; this creates additional for some employees that cannot be easily alleviated by other end users because of the restrictions on the authority of each role.

Control. Control misfits occur when the controls embedded in the system are so strict that they constrain productivity or, on the contrary, are so weak that they do not allow adequate monitoring of the performance of a function. A control deficiency may occur when the system rules would require too much unproductive work for little control benefit (e.g. moving inventories back and forth from the warehouse). In contrast, a control imposition misfit may occur when stringent system controls cause production delays.

Organisation and Culture. The final category relates to organisational and culture misfits. Tan et al. (1998) show significant differences between individualistic (US) and collectivistic (Singapore) cultures and their results are further confirmed regarding other Asian countries (Soh et al., 2000; Davison, 2002; Martinsons, 2004). Nevertheless, the adoption of information systems may conflict also with organisational culture (Markus, 2004). In the context of organisational misfits, there are only impositions. This type of misfits is particularly challenging because it can require modification of the company culture as well as the relationship between organisational functions. Indeed, information systems typically place more focus on finance and financial controls and this might create significant internal frictions that need to be addressed.

User Resistance Challenges

One of the main reasons for information systems project failures is user resistance (Keen, 1981; Markus, 1983; Krasner, 2000). User resistance should not be ignored since minor resistance can reduce the speed of change, but major resistance can lead management to abandon the project. There are different levels of resistance behaviours, and, therefore, potential consequences. Users can decide to not adopt the new system (Joseph, 2005), to not cooperate, to sabotage the project (Carnall, 1986), or even to engage in physically destructive actions (Marakas & Hornik, 1996). Klaus & Blanton (2010) identify twelve determinants of user resistance that managers should consider in adopting information systems, and classify these factors into four categories as summarised in Table 20.1

To lower user resistance, managers should, first of all, identify the main user(s) of the system. Research shows that regarding the implementation of accounting information systems, the system adoption (i.e. acceptance) by accountants within the organisation is a key factor for a successful implementation (Pulakanam & Suraweera, 2010; Vatanasakdakul et al., 2010). As a second step, managers should carefully assess what users need and what they expect from the new system, make them aware of the key objectives of the project, and provide them with adequate support, in particular during the early stage of the adoption.

[insert Table 20.1 about here]

Organisational/environment perspective

The definition of successful implementation of an information system rests mostly on subjective evaluation, and depends on the context of application (Heeks, 2002). In deciding whether to adopt an information system, and which system to implement, management should assess the alignment between the organisation's information and business strategy (Henderson & Venkatraman, 1993; Parker & Benson, 1989; Davenport, 1998; Belfo & Trigo 2013). According to Smits et al. (2003), managers should examine (at least) six factors which define the organisation competitive environment. These include the organisation's position in the industry, distribution channels, special events (e.g. mergers and acquisitions), organisation size, the degree of organisation innovativeness and the presence of an existing legacy information system. These factors all impact the decision-making process and risk profile for information systems implementation.

The sector (public vs private) in which the organisation operates has also been found to have a significant effect on its culture. According to Bannister (2001), there are many important

organisational differences between the public sector and private sector in terms of culture, structure, technology and resources. Public sector projects, for example, tend to have the following characteristics: large scale, unproven technology, hierarchical and bureaucratic decision-making and are often implemented as a result of statutory, parliamentary or supranational regulations (Jones, 2008). Furthermore, such projects are usually shaped by strong political factors (Introna, 1997; Gauld, 2007). As a consequence, the differences in terms of management's incentives, objectives and leverages in the public and private sector should lead towards different information strategies.

Heeks (2002) suggests that the country or regions in which an information system will be implemented may also impact its potential success. Historically, information systems were designed in developed countries (Barrett et al., 2001), but the contexts of the designers and end users may be very distant in physical, cultural and economic ways (Heeks, 2002). Heeks (2002) argues that the gap between design and reality (i.e. *design-actuality gap*) is the main reason behind the high failure rate in information system implementation projects in developing countries and suggests that management should pay attention to three main factors in adopting a new information system in these contexts. First, the flexibility of the system. The system should not embed too many assumptions about users' roles and activities' organisation. Second, the potential for customisation. System customisations may lead to a better fit between the organisation and the system itself. Third, the availability of local resources since the involvement of people who know both the system and the local reality is essential for project success.

Outsourcing Challenges

Outsourcing is generally defined as the commissioning of third party management of IT assets/activities to required result (Willcocks & Lester, 2000). As of the early 1990s, management and accounting scholars have endorsed outsourcing as a promising business strategy (Bardi & Tracey, 1991; Sonnenberg, 1992; Apte & Mason, 1995; Lei & Hitt, 1995; Anderson & Sedatole, 2003; Christ et al., 2014). There is a general argument that organizations should focus on their core competencies and outsource all other activities to optimise the resource allocation (Lambert & Peppard, 2013). Famous companies (e.g. AstraZeneca, Procter & Gamble and Texas Instruments[2]) have successfully outsourced part of or their entire manufacturing processes generating significant operational efficiencies.

Outsourcing AIS, or information systems more generally, is a more recent trend. Technological advancements have significantly improved the extent, speed, and reliability of global communications and have made easier to outsource critical activities (Levy, 2005; Blinder, 2006; Contractor et al., 2010; Stratman 2008). As a result, outsourcing information systems has become a common business practice (Jay, 2009; Fitoussi & Gurbaxani, 2012; Han & Mithas, 2013) and its trend is still upward.

Despite the growing importance of outsourcing in the IT domain, and despite the lower technology barriers, outsourcing AIS still represents a significant challenge for both users and providers. Indeed, the decision to outsource accounting information systems generates significant and specific risks that can be classified into three broad categories:

Relational risk. This is the risk that the partnership fails due to poor cooperation and opportunistic behaviour (Das & Teng, 1996). Relational risk arises mainly because of the intangible nature of information (Christ et al., 2014). Indeed, deliverables are hard to define and difficult to measure, thus creating an adequate contractual regime and monitoring it over the implementation period represent a real challenge (Banker et al., 2006). Furthermore, opportunistic behaviours may arise when a user

[2] See Heric & Singh (2010) and George (2012) for further details.

become too dependent from its provider (i.e. lock-in) and the latter takes advantage of the situation by increasing service price or lowering service quality (Aron & Liu, 2005).

Performance risk. This is the risk that operational or performance factors undermine the success of the partnership despite full cooperation among partners (Das & Teng, 1996). Difficulties in defining what the expected deliverables are and how to measure their quality lead to an increase in performance risk. The risk of misunderstanding between users and providers and, therefore, the risk of failure are significantly higher in this situation (Michell and Fitzgerald, 1997; Willcocks & Lacity, 1999,). Furthermore, accounting information system management requires extensive implicit knowledge (Leonardi & Bailey, 2008). Such knowledge is typically difficult to transfer and the sharing process may requires long time, significant effort and strong commitment to both users and providers as well as the alignment of their objectives. Finally, performance risk also rises when the function is off-shored, when a user engages multiple service providers (Bierstaker et al., 2013) or when the service provider does not have the expertise, sophistication, experience, or knowledge of the user's business (Christ et al., 2014).

Compliance and regulatory risk. This is the risk that the user fails to adhere to regulatory standards because of provider's errors (Anderson et al., 2014). Outsourcing accounting information systems involves sharing data, lowering control over the outsourced system and relying upon information generated by a third party (Christ et al., 2014). Compliance and regulatory risks are particularly high in this context since the user remains responsible for the work performed by the provider and inaccurate or non-compliant data may result in fines and penalties (Christ et al., 2014). In addition to regulatory penalties, reporting irregularities may cause a loss in terms of company reputation and value (Dechow et al., 1996), making the potential consequences of non-compliance even worse.

Mitigating these risks is a main concern of companies willing to outsource their accounting information systems and three key factors may provide a significant contribution towards such achievement (Blaskovich & Mintchik, 2011; Christ et al., 2014). Firstly, managers should adopt a strategic approach to outsourcing. Investing time in clarifying expectations, choosing appropriate monitoring tools, and defying long-term objectives may prevent future pains (Saunders et al., 1997; Osei-Bryson & Ngwenyama, 2006). Secondly, the selection of the right provider is key and managers should evaluate both its business specific knowledge and past experiences (Lee & Kim, 1999; Lee, 2001). Thirdly, effective communication and knowledge sharing between partners may make it easier to align their objectives and to implement effective monitoring mechanisms (Lee, 2001, Bandyopadhyay & Pathak, 2007, Han et al., 2008).

Emerging Challenges

The last decade has seen the emergence and increasing adoption of digital technologies that have resulted in ubiquitous access to the Internet for billions of users and generate an unprecedented volume of data. For enterprises, there are much cited benefits in the adoption of some of these technologies such as cloud computing, big data analytics and mobile computing however there are new challenges and risks to overcome in order to garner the value promised by them. This section discusses some of the challenges presented by cloud computing, big data and mobile working.

Cloud Computing

Cloud computing represents a horizontal technology that enables a number of other digital applications and has emerged as one of the major paradigms in information systems research and practice. Cloud computing represents a convergence of two major trends in information technology (Kim, 2009):

- IT efficiency, whereby modern computers are utilised more efficiently via highly scalable distributed hardware and software resources.
- Business agility, whereby IT can be used as a competitive tool through rapid deployment, parallel batch processing, use of computer-intensive business analytics and mobile interactive applications that respond in real time to consumer requirements.

The US National Institute of Standards and Technology (NIST) defines cloud computing as:

> "…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance 2011).

The NIST definition of cloud computing refers to three service models Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud) (Mell & Grance, 2011). Organisation of all sizes and sectors are adopting cloud computing to exploit the advantages of the agility and scalability (up and down) inherent in cloud computing (Sclater, 2009; Sultan, 2010; Lian et al., 2013; Oliveira et al., 2014). Commonly cited benefits include work efficiencies, reduced IT costs (including IT capital expenditure, maintenance and support costs and related environmental costs), business continuity and scalability (Buyya et al., 2009; Hogan et al., 2011; Low et al., 2011). Unsurprisingly, a wide variety of software vendors have adopted cloud computing across the range of software functions including sales and marketing (Salesforce.com, Hubspot, Marketo), HR (Oracle Taleo, SAP Successfactors, Workday) and of course, accounting (Xero, Big Red Book, Sage Live).

Despite the many perceived and actual benefits, cloud computing provides unique implementation challenges and perceived barriers to adoption. These include general technological challenges (migration, interoperability and portability), security, data protection and ICT governance, and contractual issues (Leimbach et al., 2014). We will discuss these now in some detail.

Technological Challenges

There are a number of technological challenges for those seeking to exploit cloud computing which largely revolve around migration to a cloud service, between cloud services and off a cloud service (Church et al., 2020). Many organisations make use of legacy systems either developed entirely within an organisation or extended and customised from a generic software base over a period of time. The extent of customisation and/or embeddedness of these systems with other software systems or organisation processes can make it challenging both technologically and culturally to migrate to the cloud. Andrikopoulos et al. (2012) present four primary strategies for migration to the cloud which present their own challenges:

- Replace components with cloud offerings;
- Partially migrate some of the application functionality to the Cloud;
- Migrate the whole software stack of the application to the Cloud;
- Cloudify the application: a complete migration of the application takes place.

At a more granular level, enterprises will face technological challenges at different layers within their information systems stack whether it is the data, business or presentation layer. Migrating the database layer of an application may result in incompatibilities with the legacy database layer (including schema, consistency models, and support for ACID transactions), synchronicity and the accidental disclosure of confidential data (Andrikopoulos et al., 2012). These may have a significant

impact on the business layer and ultimately the presentation layer. While there is an established literature base on adapting business processes, managing dependencies between cloud computing architectures and other architectures can introduce challenges. Due to the enterprise scope and complexity of most information systems, and in particular accounting information systems, it is difficult to generate an integrated migration model so that dependencies on components being moved to the cloud can be identified. Discovering, creating and maintaining such a model can be significant challenges in themselves. Once a model has been created, the services and supporting infrastructure to migrate must be (i) identified, (ii) extracted, (iii) adapted and optimised, (iv) deployed to the Cloud, and (iv) removed from the source environment. This must be done with the least impact possible on operations and ideally with improvement to performance post-migration.

The logical and physical distribution of a migrated application also provides significant challenges (Andrikopoulos et al., 2012). These include regional variances in data protection compliance, performance and cost (Reese, 2009; Schad et al., 2010). Scalability, a much cited advantage of cloud computing, is not without challenges. Horizontal scaling, adding more instances as required, depends on the application components and the application as a whole to support it as an option, the complexity of which is exacerbated where there is high transactionality such as in an accounting information system (Andrikopoulos et al., 2012). What, how, when and how much to scale are application-specific challenges for IS decision-makers to consider.

Migrating from one cloud provider to another is challenging due to a lack of standards in interoperability and portability. Interoperability issues may arise between and within layers (Pahl et al., 2013). Both the lack of standards and lack of adoption of existing standards by cloud service providers exacerbates the issue (Nguyen et al., 2012). Indeed, it may not be in the best interest of cloud service providers to adopt standards and common application models. Designing an application for optimal performance on a specific cloud infrastructure may result in lock-in to that cloud service provider, thereby negating the flexibility cloud computing purports to offer. As a result, a future portability issue is created when the customer wishes to migrate from one cloud service provider to another or indeed repatriate from the cloud. Whereas this is a disadvantage to the customer, it has strategic value to the service provider.

Security Issues in Cloud Computing

Each of the three cloud computing service models has their own security issues (Kandukuri & Rakshit, 2009). The SaaS deployment model is the most widely used by enterprise IT services involving the software vendors deploying their software applications remotely in the cloud and accessible via the Internet. For the most part, the cloud service provider is responsible for security function. Subashini & Kavitha (2011) identify 13 security elements that need to be considered in SaaS. These are summarised in Table 20.2.

Enterprises have more control over security as they move from SaaS to PaaS and IaaS deployment models. In PaaS, any security below the application level is still the responsibility of the service provider and many of the issues in Table 20.2 still apply. At the IaaS level, the cloud service provider is often only responsible for a minimal level of security e.g. physical security, environmental security and virtualization security. As virtualization security is the only element within a developer's immediate control, care needs to be taken on assuring that there are no vulnerabilities in the virtualization manager.

[insert Table 20.2 about here]

Data Protection and ICT Governance

Cloud computing exacerbates AIS challenges with regard to data protection and ICT governance (Coss & Dhillon, 2020). Due to the distributed nature of cloud computing, the location of data in transit (during processing and storage) may not be known by the user. This raises two key challenges. Firstly, enterprises may find themselves subject to laws and regulations in unintended jurisdictions raising issues of compliance. Secondly, lack of clarity on the identity of actors raises issues of the role of various actors and associated responsibilities (and potential liabilities) under data protection legislation.

The global and distributed nature of cloud computing combined with dominance by US firms introduces significant challenges from an ICT governance perspective. In particular, there is currently widespread uncertainty between data protection regimes in the US and the European Union. This relates to the debate on actions of intelligence agencies, and specifically the US intelligence community, and their ability and actions to require telecommunications service providers to store and provide access to data under a valid court order. Such disclosure may or may not be revealed to the ultimate owners of the data. This jurisdictional ambiguity may result in compliance issues, increasing both financial and legal risks to the firm.

From an accounting perspective, existing regulations relating to the management and auditing of internal control frameworks for information technologies and systems are pertinent in the context of the use of accounting information systems in the cloud – for example, Statement of Auditing Standards (SAS) No. 70 and Statement on Standards for Attestation Engagements (SSAE) No. 16. Commentators have highlighted the need under international standards for auditors to understand a firm's business processes and internal controls in order to complete a thorough risk assessment of these processes, controls and indeed the financial statements (Singleton, 2010; Alali & Yeh, 2012; Smith et al., 2019).

Contractual Issues in the Cloud

Cloud computing introduces a range of high-level contractual issues (see Table 20.3) which in themselves provide challenges for enterprises seeking to implement systems in the cloud. Cloud computing contracts typically are made up of one or more of the following documents (Bradshaw et al., 2011; Leimbach et al., 2014; Lynn, 2021):

- Terms of Service (provisions regarding the overall relationship between parties).
- Service Level Agreement (details regarding the level of service to be provided and related penalties for not meeting agreed levels).
- Acceptable Use Policy (a policy to protect cloud service providers from the actions of clients or customers of clients).
- Privacy Policy (the cloud service provider's policy for handling and protecting data).

The negotiation of cloud service contracts is a relatively rare event, often limited to the largest organisations (Bradshaw et al., 2011; Leimbach et al., 2014; Opara-Martins et al., 2014). Yet,

contracts can be a source of risk and friction for firms adopting the cloud resulting in a loss of control and/or contractual lock-in.

[insert Table 20.3 about here]

Big Data

Big data is a sobriquet for datasets that are characterised by scale differences in volume (size), velocity (rate), and variety (range of formats and representations) than conventional datasets and as such conventional, data processing infrastructure, applications and tools are often found inadequate (Laney, 2001). Today, big data is driven by increased connectivity and usage of Internet-based systems and devices, accelerated by cloud computing and social media amongst other technologies. From an accounting perspective, big data is generated not only by the volume of transactions and related operations within a firm but the increasing volume of machine-generated data (including the so-called 'Internet of Things'), metadata and supplemental and complementary data available from internal and third-party sources (Vasarhelyi et al., 2015). Commentators suggest that this additional big data and the ability to analyse it to make decisions has the potential to dramatically improve corporate performance across all functions (LaValle et al., 2011; Manyika et al., 2011). From an accounting perspective, big data provides additional data and evidence to assist management in making decisions. As such, it has the potential of impacting a wide range of accounting related functions including the audit function, business measurement, and business intelligence (Moffitt & Vasarhelyi, 2013; Vasarhelyi et al., 2015,).

With the widespread use of cloud computing infrastructure for big data analytics, it is unsurprising that many of the challenges of cloud computing are shared with big data implementations. However, big data, by its nature, provides new challenges driven by the size and complexity of the datasets and the technologies needed to process such datasets (Ward & Barker, 2013). These include new embedded architectures and systems that can both manage and scale with data as it grows including internal ICT governance and data management infrastructure and processes (LaValle et al., 2011). Designing and migrating to such an architecture is a major challenge. Big data involves a specialist set of analytical technologies, tools and techniques that can handle both structured and unstructured data and generate insights from such data (Lynn et al., 2015). Such infrastructure can be extremely costly from a computational perspective and such toolsets are still at an early stage of development with significant issues even in terms of analytical validity. The high dimensionality and sample size of big data can result in noise accumulation, spurious correlations, and incidental homogeneity while at the same time, heterogeneity issues caused from multiple sources, time points and biases (Fan et al. 2014). As such, firms seeking to exploit big data require not only analysts who can understand their business but data scientists and ideally a combination of both. Unsurprisingly, there is a significant shortage in the labour market of such personnel (Manyika et al,. 2011). As this shortfall is unlikely to be filled in the near future, some have argued that the accountants' mindset lends itself to such bimodal thinking and data-driven analysis, however a significant upskilling would be required (Bhimani & Wilcocks, 2014).

While big data promises enterprises greater insights and ultimately value, it also represents a significant challenge for internal controls and specifically data protection and compliance. The value of such data increases the likelihood for large-scale theft and/or breaches related to sensitive data in the form of unauthorised access for financial gain, intelligence or merely to compromise the interpretation/analysis process (Fhom, 2015). In addition to security, there is widespread concern from policymakers in relation to individual control over personal data and related issues regarding the provenance of data and consent management (Fhom, 2015; Leimbach et al., 2014). While these might be considered ethical and social challenges, they have very real implications for those responsible for internal controls particularly where such data is integrated into accounting information

systems. Accounting and financial professionals, including auditors, may face increasing pressure and scrutiny from policymakers and regulators to ensure adequate controls are in place to protect such big data (Huerta & Jensen, 2017).

Mobile Working and Bring Your Own Technology

Increasingly employees and customers have ubiquitous access to the Internet. Technological advances in mobile broadband, combined with widespread adoption of cloud computing and social media, have driven extremely high penetration and usage of mobile devices, and specifically smartphones and tablets. Major software vendors, including those in ERP and accounting software, typically have mobile access offerings. Mobile computing provides a wide range of benefits covered extensively in the teleworking literature (Baruch, 2000; Morgan, 2004). However, like outsourcing and cloud computing, it redefines the organisational boundaries and thus creates challenges particularly in relation to security and control. Lost devices, theft, security vulnerabilities in mobile access networks, devices, apps and devices are just some of the challenges to enterprises supporting enterprise mobile computing (Harris & Patten, 2014; Romer 2014).

A particular phenomenon worth noting is "BYOD" or "Bring Your Own Device" which refers to employees using their own hardware to access company's information. However, to limit it to devices is a misnomer. People are not only bringing their own hardware but increasingly software too; "Bring Your Own Technology" or "BYOT" is more appropriate (Miller et al., 2012). The trade press has popularised the benefits of the BYOT phenomenon including teleworking, technology familiarity, improved morale, increased access and availability of employees, increased working hours and reduced cost (Boomer, 2012; Chaudry, 2012; Singh, 2012). However, BYOT also introduces security and internal control risks. Here security is an afterthought; the employee has not bought the device for enterprise security but for a range of personal motivations (Morrow, 2012; Romer, 2014). "Personal" is a very important attribute of BYOT. As a result of personal decisions, the enterprise risks change and intensify. Lost devices, data contamination, new forms of malware, phishing attack success, and risky file sharing become more likely (Miller et al., 2012; Morrow, 2012; Romer, 2014). The personal nature of the technology in BYOT scenarios undermines enterprise control and transparency over data to an unprecedented scale introducing new management, control and compliance complexities (Crossler et al., 2014).

During the COVID-19 pandemic, remote working from home became the norm for many worldwide. While this undoubtedly contributed significantly to business and economic continuity, it highlighted the unpreparedness of organisations and individuals for home working and the associated cybersecurity threats (Furnell & Shah, 2020). As well as a rise in home working, there was a significant increase in cybercrime attempts including scams and phishing, malware, and distributed denial of service (DDOS) attacks (Pranggono & Arabo, 2020). The COVID-19 pandemic has highlighted the need for robust cybersecurity risk management processes and cyber-literacy in general but specifically for AIS given the sensitive nature of the information stored on these systems and for their critical role within the day-to-day business operations.

Conclusion

Challenges to the adoption and successful implementation of accounting information systems are not dissimilar to those in other enterprise contexts. Enterprises face many of the same challenges that feature in the general information systems academic literature namely project management, technology, user resistance, organisation/environment and outsourcing challenges. Due to the sensitive nature of accounting information, trends towards outsourcing and the extended enterprise accelerated by the emergence of cloud computing, provide specific challenges for enterprises as they redefine their organisational boundaries and grapple with control and compliance issues associated

with such strategies. Increased mobility and the BYOT phenomenon only further complicate enterprise management of mission-critical and sensitive systems. The emergence of big data provides similar but also different challenges for accounting and financial professionals. It is not difficult to foresee a time in the very near future where big data, whether sourced from internal or external sources, will become a major component of the business intelligence, business measurement and audit evidence activities of enterprises. Together and individually, cloud computing, big data and mobile computing are transforming business processes and creating new competitive advantages. Whilst the changes to accounting and auditing processes, systems and standards has not integrated these technologies at the same pace as other enterprise functions, greater focus by practitioners and researchers are required if only to reduce risk.

References

Addison, T. & Vallabh, S. (2002). Controlling software project risks: an empirical study of methods used by experienced project managers, *Proceedings of the 2002 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, 2002. South African Institute for Computer Scientists and Information Technologists, 128-140.

Alali, F.A. & Yeh, C.L. (2012). Cloud computing: Overview and risk analysis. *Journal of Information Systems*, 26(2), 13-33.

Aloini, D., Dulmin, R. & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature, *Information & Management,* 44(6), 547-567.

Anderson, S. W., Christ, M. H., Dekker, H. C. & Sedatole, K. L. (2014). The use of management controls to mitigate risk in strategic alliances: Field and survey evidence, *Journal of Management Accounting Research,* 26(1)**,** 1-32.

Anderson, S. W. & Sedatole, K. L. (2003). Management accounting for the extended enterprise: Performance management for strategic alliances and networked partners, in Bhimani A., ed., *Management accounting in the digital economy*, Oxford:Oxford University Press.

Andrikopoulos, V., Binz, T., Leymann, F. & Strauch, S. (2013). How to adapt applications for the Cloud environment, *Computing*, 95(6), 493-535.

Apte, U. M. & Mason, R. O. (1995). Global disaggregation of information-intensive services, *Management science,* 41(7)**,** 1250-1262.

Aron, R. & Liu, Y. (2005). Determinants of operational risk in global sourcing of financial services: Evidence from field research, *Brookings Trade Forum*, 1, 373-398.

Bandyopadhyay, S. & Pathak, P. (2007). Knowledge sharing and cooperation in outsourcing projects—A game theoretic analysis, *Decision Support Systems,* 43(2)**,** 349-358.

Banker, R. D., Kalvenes, J. & Patterson, R. A. (2006). Research note-information technology, contract completeness, and buyer-supplier relationships, *Information Systems Research*, 17(2), 180-193.

Bannister, F. (2001). Dismantling the silos: extracting new value from IT investments in public administration, *Information Systems Journal,* 11(1), 65-84.

Bardi, E. J. & Tracey, M. (1991). Transportation outsourcing: a survey of US practices, *International Journal of Physical Distribution & Logistics Management,* 21(3), 15-21.

Barrett, M., Sahay, S. & Walsham, G. (2001). Information technology and social transformation: GIS for forestry management in India, *The Information Society,* 17(1), 5-20.

Baruch, Y. (2000). Teleworking: benefits and pitfalls as perceived by professionals and managers. New Technology, *Work and Employment*, 15(1), 34–49.

Belfo, F. & Trigo, A. (2013). Accounting information systems: tradition and future directions, *Procedia Technology,* 9, 536-546.

Bhimani, A. & Willcocks, L. (2014). Digitisation,Big Dataand the transformation of accounting information. *Accounting and Business Research*, 44(4), 469-490.

Bierstaker, J., Chen, L., Christ, M. H., Ege, M. & Mintchik, N. (2013). Obtaining assurance for financial statement audits and control audits when aspects of the financial reporting process are outsourced, *Auditing: A Journal of Practice & Theory,* 32(1), 209-250.

Blaskovich, J. & Mintchik, N. (2011). Information technology outsourcing: A taxonomy of prior studies and directions for future research, *Journal of Information Systems,* 25(1), 1-36.

Blinder, A. S. (2006). Offshoring: the next industrial revolution?, *Foreign Affairs*, 85(1), 113-128.

Boehm, B. W. (1981). An experiment in small-scale application software engineering, *IEEE Transactions on Software Engineering,* 7(5), 482-493.

Boomer, J. (2012). Are you ready for BYOD, *CPA Practice Advisor*, May 28, available from: h https://www.cpapracticeadvisor.com/directory/business-management/article/10707592/are-you-ready-for-byod [15 August 2021].

Borcherding, J. D., Samelson, N. M. & Sebastian, S. M. (1980). Improving motivation and productivity on large projects, *Journal of the Construction Division,* 106(1), 73-89.

Bradshaw, S., Millard, C. and Walden, I. (2011). Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. *International Journal of Law and Information Technology*, 19(3), 187-223.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future Generation computer systems,* 25(6), 599-616.

Carnall, C. A., (1986). Managing strategic change: An integrated approach, *Long Range Planning,* 19(6), 105-115.

Cervone, H. F. (2006). Project risk management, *OCLC Systems & Services: International digital library perspectives,* 22(4), 256-262.

Chapman, C. & Ward, S. (2003). *Project risk management: processes, techniques and insights,* Hoboken, NJ: John Wiley & Sons.

Chaudhry, P. (2012). Tech strategy—Needed: A corporate mobile device policy, *Magazine of Financial Executive Institute*, 28(5), 69.

Christ, M. H., Mintchik, N., Chen, L. & Bierstaker, J. L. (2014). Outsourcing the Information System: Determinants, Risks, and Implications for Management Control Systems, *Journal of Management Accounting Research,* 27(2), 77-120.

Christen, P. (2014). Privacy Aspects in Big Data Integration: Challenges and Opportunities. In *Proceedings of the First International Workshop on Privacy and Security of Big Data*, Shangai, 1-1.

Church, K.S., Schmidt, P.J. & Ajayi, K. (2020). Forecast Cloudy—Fair or Stormy Weather: Cloud Computing Insights and Issues. *Journal of Information Systems*, 34(2), 23-46.

Contractor, F. J., Kumar, V., Kundu, S. K. & Pedersen, T. (2010). Reconceptualizing the firm in a world of outsourcing and offshoring: The organizational and geographical relocation of high-value company functions, *Journal of Management Studies,* 47(8), 1417-1433.

Coss, D.L. & Dhillon, G. (2020). A framework for auditing and strategizing to ensure cloud privacy. *Journal of Information Systems*, 34(2), 47-63.

Crossler, R.E., Long, J.H., Loraas, T.M. & Trinkle, B.S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap, *Journal of Information Systems*, 28(1), 209-226.

Das, T. & Teng, B. S. (1996). Risk types and inter-firm alliance structures, *Journal of Management Studies,* 33(6), 827-843.

Davenport, T. H. (1998). Putting the enterprise into the enterprise system, *Harvard Business Review,* 76(4). 1-11.

Davison, R. (2002). Cultural complications of ERP, *Communications of the ACM,* 45(7), 109-111.

Dechow, N. & Mouritsen, J. (2005). On enterprise wide resource planning systems-the quest for integration and management control, *Accounting, Organizations and Society,* 30(7), 691–733.
Dechow, P. M., Sloan, R. G. & Sweeney, A. P. (1996). Causes and consequences of earnings manipulation: An analysis of firms subject to enforcement actions by the SEC, *Contemporary Accounting Research,* 13(1), 1-36.
Elliott, B. (2007). Anything is possible: Managing feature creep in an innovation rich environment, *Proceedings of the Engineering Management Conference*, Singapore, 304-307.
Ewusi-Mensah, K. (1997). Critical issues in abandoned information systems development projects, *Communications of the ACM*, 40(9), 74-80.
Fan, J., Han, F. and Liu, H. (2014). Challenges of big data analysis. *National Science Review*, 1(2), 293–314.
Fitoussi, D. & Gurbaxani, V. (2012). IT outsourcing contracts and performance measurement, *Information Systems Research,* 23(1), 129-143.
Fhom H.S. (2015). Big Data: Opportunities and Privacy Challenges, in Richter, P., *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data*, 13-44. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.
Fraser, S. D., Brooks Jr, F. P., Fowler, M., Lopez, R., Namioka, A., Northrop, L., Parnas, D. L. & Thomas, D. (2007). No silver bullet reloaded: retrospective on essence and accidents of software engineering, *Companion to the 22nd ACM SIGPLAN conference on Object-oriented programming systems and applications companion*, Montreal, 1026-1030.
Fui-Hoon Nah, F., Lee-Shang Lau, J. & Kuang, J. (2001). Critical factors for successful implementation of enterprise systems, *Business Process Management Journal,* 7(3), 285-296.
Furnell, S. & Shah, J.N. (2020). Home working and cyber security–an outbreak of unpreparedness?. *Computer Fraud & Security*, (8), 6-12.
Gattiker, T. F. & Goodhue, D. L. (200). What happens after ERP implementation: undersanding the impact of interdependence and differentiation on plant-level outcomes, *MIS Quarterly*, 29(3), 559-585.
Gauld, R. (2007). Public sector information system project failures: Lessons from a New Zealand hospital organization, *Government Information Quarterly*, 24(1), 102-114.
George, B. (2012). Best Practices in Outsourcing: The Procter & Gamble Experience. *IAOPs Global Excellence in Outsourcing Award.* Available from: https://www.iaop.org/Download/Download.aspx?ID=1920. [15 August 2021].
Grabski, S. V., Leech, S. A. & Schmidt, P. J. (2011). A review of ERP research: A future agenda for accounting information systems, *Journal of Information Systems,* 25(1), 37-78.
Han, H.-S., Lee, J.-N. & Seo, Y.-W. (2008). Analyzing the impact of a firms capability on outsourcing success: A process perspective, *Information & Management,* 45(1), 31-42.
Han, K. & Mithas, S. (2013). Information Technology Outsourcing and Non-IT Operating Costs: An Empirical Investigation, *MIS Quarterly,* 37(1), 315-331.
Harris, M. & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. I*nformation Management & Computer Security,* 22(1), 97–114.
Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations, *The Information Society,* 18(2), 101-112.
Henderson, J. C. & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations, *IBM Systems Journal,* 32(1), 4-16.
Heric, M. & Singh, B. (2010). Outsourcing Can Do Much More Than Just Cut Costs. *Forbes*, 15 June, available from: http://www.forbes.com/2010/06/15/outsourcing-capability-sourcing-leadership-managing-bain.html [Accessed 15 August 2021].
Hogan, M., Liu, F., Sokol, A. & Tong, J. (2011). Nist cloud computing standards roadmap, *NIST Special Publication,* 35.
Huerta, E. & Jensen, S. (2017). An accounting information systems perspective on data analytics and Big Data. *Journal of Information sSstems*, *31*(3), 101-114.

Introna, L. (1997). *Management, Information and Power: A narrative of the involved manager,* London:Macmillan.

Jay, J. (2009). Pricing and Valuation Services: The Search for Transparency. AITE Group, LLC, 11 November, available from: http://aitegroup.com/report/pricing-and-valuation-services-search-transparency. [15 August 2021].

Jones, S. (2008). Social dimension of IT/IS evaluation: Views from the public sector, in Irani, Z. & Love, PED, *Evaluating information systems: Public and private sector.* London: Routledge 236-256.

Joseph, R. C. (2005). To Adopt or Not to Adopt - That is the Question, *Proceedings of Americas Conference on Information Systems (AMCIS)*, Omaha, 1219-1224.

Kandukuri, B. R. & Rakshit, A. (2009). Cloud security issues, *Proceedings of the 2009 IEEE International Conference on Services Computing*, Bangalore, 517-520.

Keen, P. G. (1981). Information systems and organizational change, *Communications of the ACM,* 24(1), 24-33.

Khurana, A. & Rosenthal, S. R. (1997). Integrating the fuzzy front end of new product development, *MIT Sloan Management Review*, 38(2), 103-120.

Kim, W. (2009). Cloud Computing: Today and Tomorrow, *Journal of Object Technology,* 8(1), 65-72.

Klaus, T. & Blanton, J. E. (2010). User resistance determinants and the psychological contract in enterprise system implementations, *European Journal of Information Systems*, 19(6), 625-636.

Krasner, H. (2000). Ensuring e-business success by learning from ERP failures, *IT Professional,* 2(1), 22-27.

Lakhanpal, B. (1993). Understanding the factors influencing the performance of software development groups: An exploratory group-level analysis, *Information and Software Technology,* 35(8), 468-473.

Lambert, R. & Peppard, J. (2013). The Information Technology–Organizational Design Relationship, in Galliers, RD & Leidner, DE, *Strategic Information Management*, London: Routledge, 427-459.

Laney, D. (2001). 3D data management: controlling data volume, velocity and variety. META Group Research Note, 6, 70.

Landis, L., Waligora, S., Mcgarry, F., Pajerski, R., Stark, M., Johnson, K. O. & Cover, D. (1992). Recommended approach to software development, revision 3, National Aeronautics and Space Administration (NASA), June. Available from: http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19930009672.pdf. [15 August 2021].

Larson, C. E. & LaFasto, F. M. (1989). *Teamwork: What must go right, what can go wrong.* Newberry Park, CA:Sage.

Laumer, S. & Eckhardt, A. (2012). Why do people reject technologies: a review of user resistance theories, in Dwivedi, YK, Wade, MR, & Schneberger, SL., *Information Systems Theory*, 63-86. Springer, New York.

LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S. & Kruschwitz, N. (2011). Big data, analytics and the path from insights to value, *MIT Sloan Management Review*, 52(2), 21-32.

Lee, J.-N. (2001). The impact of knowledge sharing, organizational capability and partnership quality on IS outsourcing success, *Information & Management,* 38(5), 323-335.

Lee, J.-N. & Kim, Y.-G. (1999). Effect of partnership quality on IS outsourcing success: conceptual framework and empirical validation, *Journal of Management Information Systems*, 15(4), 29-61.

Lei, D. & Hitt, M. A. (1995). Strategic restructuring and outsourcing: The effect of mergers and acquisitions and LBOs on building firm skills and capabilities, *Journal of Management*, 21(5), 835-859.

Leimbach, T., Hallinan, D., Bachlechner, D., Weber, A., Jaglo, M., Hennen, L., Nielsen, R.Ø., Nentwich, M., Strauß, S., Lynn, T. & Hunt, G. (2014). Potential and Impacts of Cloud Computing Services and Social Network Websites, Science and Technology Options Assessment (STOA). Available from: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf. [15 August 2021].

Leonardi, P. M. & Bailey, D. E. (2008). Transformational technologies and the creation of new work practices: Making implicit knowledge explicit in task-based offshoring, *MIS Quarterly*, 411-436.

Levy, D. L. (2005). Offshoring in the new global political economy, *Journal of Management Studies,* 42(3), 685-693.

Lian, K.-Y., Hsiao, S.-J. & Sung, W.-T. (2013). Intelligent multi-sensor control system based on innovative technology integration via ZigBee and Wi-Fi networks, *Journal of Network and Computer Applications,* 36(2), 756-767.

Low, C., Chen, Y. & Wu, M. (2011). Understanding the determinants of cloud computing adoption, *Industrial Management & Data Systems,* 111(7), 1006-1023.

Lynn, T., Healy, P., Kilroy, S., Hunt, G., Van Der Werff, L., Venkatagiri, S., & Morrison, J. (2015). Towards a general research framework for social media research using big data. I*n IEEE International Professional Communication Conference (IPCC*) (1-8). IEEE.

Lynn, T. (2021). Dear Cloud, I Think We Have Trust Issues: Cloud Computing Contracts and Trust. In *Data Privacy and Trust in Cloud Computing* (21-42). Cham: Palgrave Macmillan.

Lyytinen, K. & Robey, D. (1999). Learning failure in information systems development, *Information Systems Journal*, 9(2), 85-101.

Maier, C., Laumer, S., Eckhardt, A. & Weitzel, T. (2013). Analyzing the impact of HRIS implementations on HR personnels job satisfaction and turnover intention, *The Journal of Strategic Information Systems,* 22(3), 193-207.

Malhotra, N., Bhardwaj, M. & Kaur, R. (2012). Estimating the effects of gold plating using fuzzy cognitive maps, *International Journal of Computer Science and Information Technologies,* 3(4), 4806-4808.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. & Byers, A.H. (2011). Big data: The next frontier for innovation, competition, and productivity, Mckinsey Global Institute, May, available from: http://www.mckinsey.com/business-functions/business-technology/our-insights/big-data-the-next-frontier-for-innovation. [15 August 2021].

Marakas, G. M. & Hornik, S. (1996). Passive resistance misuse: overt support and covert recalcitrance in IS implementation, *European Journal of Information Systems*, 5(3), 208-219.

Markus, M. L. (1983). Power, politics, and MIS implementation, *Communications of the ACM*, 26(6), 430-444.

Markus, M. L. (2000). Paradigm shifts-e-business and business/systems integration, *Communications of the Association for Information Systems*, 4(1), Article 10.

Markus, M. L. (2004). Technochange management: using IT to drive organizational change, *Journal of Information Technology*, 19(1), 4-20.

Martinsons, M. G. (2004). ERP in China: one package, two profiles, *Communications of the ACM,* 47(7), 65-68.

McConnell, S. (1996). *Rapid development: taming wild software schedules.* London: Pearson Education.

McConnell, S. (2006). *Software estimation: demystifying the black art,* Microsoft Press.

Mell, P. & Grance, T. (2011). The NIST definition of cloud computing, *National Institute of Standards and Technology (NIST)*, September. Available from: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf. [15 August 2021].

Michell, V. & Fitzgerald, G. (1997). The IT outsourcing market-place: vendors and their selection, *Journal of Information Technology*, 12(3), 223-237.

Miller, K.W., Voas, J.M. and Hurlburt, G.F. (2012.) BYOD: Security and Privacy Considerations, *IT Professional*, 14(5), 53-55.
Moffitt, K.C. & Vasarhelyi, M.A. (2013). AIS in an age of big data, *Journal of Information Systems*, 27(2), 1-19.
Morgan, R. E. (2004). Teleworking: an assessment of the benefits and challenges. *European Business Review*, 16(4), 344–357.
Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, 12, 5-8.
Murray, J. P. (2001). Reducing IT project complexity, in Tinnirello, PC, ed., *New Directions in Project Management*, Boca Raton, FL: CRC Press, 435.
Nelson, R. R. (2007). IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices, *MIS Quarterly Executive*, 6(2), 67-78.
Nguyen, D. K., Lelli, F., Papazoglou, M. P. & Van Den Heuvel, W.-J. (2012). Blueprinting approach in support of cloud computing, *Future Internet,* 4(1), 322-346.
Oliveira, T., Thomas, M. & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors, *Information & Management,* 51(5), 497-510.
Opara-Martins, J., Sahandi, R. & Tian, F. (2014). Critical review of vendor lock-in and its impact on adoption of cloud computing, *Proceedings of the International Conference on Information Society (i-Society)*, 92-97.
Osei-Bryson, K.-M. & Ngwenyama, O. K. (2006). Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts, *European Journal of Operational Research*, 174(1), 245-264.
Pahl, C., Zhang, L. & Fowley, F. (2013). Interoperability standards for cloud architecture, *Proceedings of the 3rd International Conference on Cloud Computing and Services Science*, Aachen, available from: http://doras.dcu.ie/17824/1/closer13-sp.pdf. [15 August 2021].
Parker, M. M. & Benson, R. J. (1989) Enterprisewide information management: state-of-the-art strategic planning, *Information System Management*, 6(3), 14-23.
Peffers, K., Gengler, C. E. & Tuunanen, T. (2003). Extending critical success factors methodology to facilitate broadly participative information systems planning, *Journal of Management Information Systems*, 20(1), 51-85.
Pranggono, B. & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, 4(2), e247.
Pulakanam, V. & Suraweera, T. (2010). Implementing accounting software in small business in New Zealand: an exploratory investigation, *Accountancy Business and the Public Interest,* 9, 98-124.
Quattrone, P. & Hopper, T. (2005). A time–space odyssey: management control systems in two multinational organisations, *Accounting, Organizations and Society*, 30(7), 735-764.
Reese, G. (2009). *Cloud application architectures: building applications and infrastructure in the cloud.* Sebastopol, CA: OReilly Media, Inc..
Reid, S. E. & De Brentani, U. (2004). The fuzzy front end of new product development for discontinuous innovations: A theoretical model, *Journal of Product Innovation Management*, 21(3), 170-184.
Romer, H. (2014). Best practices for BYOD security, *Computer Fraud & Security*, 1, 13-15.
Saunders, C., Gebelt, M. & Hu, Q. (1997). Achieving success in information systems outsourcing, *California Management Review*, 39(2), 63-79.
Schad, J., Dittrich, J. & Quiané-Ruiz, J.-A. (2010). Runtime measurements in the cloud: observing, analyzing, and reducing variance, *Proceedings of the VLDB Endowment*, 3(1), 460-471.
Sclater, N. (2009). *Cloudworks, eLearning in the Cloud.* Cambridge, UK: The Free Press.
Singleton, T.W. (2010). IT Audit Basics: IT Audits of Cloud and SaaS, *ISACA Journal*, 3, 1-3.

Singh, N. (2012). BYOD genie is out of the bottle–"Devil or angel", *Journal of Business Management & Social Sciences Research*, 1(3), 1-12.

Smith, A.L., Zhang, Y. & Kipp, P.C. (2019). Cloud-computing risk disclosure and ICFR material weakness: The moderating role of accounting reporting complexity. *Journal of Information Systems*, 33(3), 1-17.

Smith, P. G. and Reinertsen, D. G. (1998). Developing Products in Half the Time: New Rules, New Tools. Hoboken, NJ: John Wiley & Sons.

Smits, M., van der Poel, K. & Ribbers, P. (2003). Assessment of information strategies in insurance companies, in Galliers, RD & Leidner, DE, *Strategic Information Management*, New York: Routledge, 64-88.

Soh, C., Kien, S. S. & Tay-Yap, J. (2000). Enterprise resource planning: cultural fits and misfits: is ERP a universal solution?, *Communications of the ACM*, 43(4), 47-51.

Sonnenberg, F. K. (1992). Partnering: entering the age of cooperation, *Journal of Business Strategy*, 13(3), 49-52.

Stratman, J. K. (2008). Facilitating offshoring with enterprise technologies: Reducing operational friction in the governance and production of services, *Journal of Operations Management*, 26(2), 275-287.

Strong, D. M. & Volkoff, O. (2010). Understanding Organization—Enterprise System Fit: A Path to Theorizing the Information Technology Artifact, *MIS Quarterly*, 731-756.

Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing, *Journal of Network and Computer Applications*, 34(1), 1-11.

Sultan, N. (2010). Cloud computing for education: A new dawn?, *International Journal of Information Management*, 30(2), 109-116.

Sumner, M. (1999) Critical success factors in enterprise wide information management systems projects, *Proceedings of the 1999 ACM SIGCPR conference on Computer personnel research*, New Orleans, 297-303.

Tan, B. C., Wei, K.-K., Watson, R. T., Clapper, D. L. & Mclean, E. R. (1998). Computer-mediated communication and majority influence: Assessing the impact in an individualistic and a collectivistic culture, *Management Science*, 44(1), 1263-1278.

The Standish Group (2020). *CHAOS 2020 Beyond Infinity*. Boston, Massachusetts: The Standig Group..

Umble, E. & Umble, M. (2001). Enterprise resource planning systems: a review of implementation issues and critical success factors, *Proceedings of the 32nd annual meeting of the decision sciences institute*, 1109-1111.

Vasarhelyi, M.A., Kogan, A. & Tuttle, B.M. (2015). Big data in accounting: An overview, *Accounting Horizons*, 29(2), 381-396.

Vatanasakdakul, S., Aoun, C. & Li, Y. (2010) AIS in Australia: UTAUT application and cultural implication, *Proceedings of the 21st Australasian Conference on Information Systems*, 1-11,

Volkoff, O., Strong, D. M. & Elmes, M. B. (2005). Understanding enterprise systems-enabled integration, *European Journal of Information Systems*, 14(2), 110-120.

Wailgum, T. (2009). 10 Famous ERP disasters, dustups and disappointments. *CIO Magazine*, 24 March, available from: http://www.cio.com/article/2429865/enterprise-resource-planning/10-famous-erp-disasters--dustups-and-disappointments.html. [15 August 2021].

Ward, J.S. & Barker, A. (2013). Undefined by data: a survey of big data definitions, arXiv preprint arXiv:1309.5821.

Willcocks, L. P. & Lacity, M. C. (1999). IT outsourcing in insurance services: risk, creative contracting and business advantage, *Information Systems Journal*, 9(3), 163-180.

Willcocks, L. P. & Lester, S. (2000). Information technology and organizational performance: Beyond the IT productivity paradox, in Galliers, RD & Leidner DE, *Strategic Information Management: Challenges and Strategies in Managing Information Systems.* Oxford:Butterworth-Heinemann, 588-608.

Table 20.1 Categories and determinants of user resistance in information systems projects

Category	Determinants	Description
Individual Issues	Uncertainty	Users are unclear of the future and view a new system as a potential threat to their job.
	Input	A new system is usually forced upon users without being able to contribute to the change process.
	Power	A new system can cause a loss of control or recognition as an "expert" inside the organisation.
	Self-efficacy	A new system may cause a lack of confidence in the skill set needed.
System Issues	Technical	Users are suddenly required to use a system with bugs and features that do not work, and they do not have figured 'work-arounds' to these problems.
	Complexity	Users experience confusion when using a new system, which typically consists of many modules.
Organisational Issues	Facilitating Environment	Users working in a static organisation (i.e. bureaucratic) are more likely to resist to the adoption of a new information systems since they expect (are used) to face only small incremental changes.
	Communication	Users who have not been informed about the benefits of the system and the reasons behind the change are more likely to create resistance.
	Training	Users tend to perceive training as a waste of time while it is a key element of a successful implementation.
Process Issues	Job or Skill Change	Users may be required to perform different tasks following the adoption of a new system, and it might cause a learning process which requires a certain effort.
	Workload	The adoption of a new system usually requires additional effort during the implementation and in the daily usage. This aspect is particularly detrimental if users do not feel compensated for the workload change.
	Lack of Fit	A new system may force the organisation to change the organisational structure with consequences on users' daily activities.

Table 20.2 Software-as-a-Service security issues and challenges (adapted from Subashini and Kavitha, 2011)

Security Issue	Challenge
Data security	Data residing outside the enterprise boundary is no longer subject to its physical, logical and personnel security and access control policies thus increasing risk from application vulnerabilities and malicious insiders.
Network security	All data flow between the enterprise and cloud service provider over the network needs to be secured to prevent leakage of sensitive information.
Data locality	The location of data in transit, storage and while being processed must be reliably known and secure.
Data integrity	Data integrity issues are exacerbated by the distributed and multi-tenant nature of the cloud. Issues could be introduced by lack of support for different service and availability levels for different types of transactions.
Data segregation	As data from multiple tenants is stored at the same location, data intrusion by hacking or application vulnerabilities is a risk.
Data access	In addition to security and access policies and controls for their own employees, enterprises need to consider the policies and controls of their cloud service provider.
Authentication and authorization	Enterprises must synchronise their user management not only for internal systems but all cloud services.. Identity management should be flexible and compliant with enterprise policies. Credentials should be secure in-transit and storage. Trust relationships and validations should be established where federation is used.
Data confidentiality	Use of cloud computing may result in perceived or actual disclosure of personal or confidential data to the cloud service provider potentially resulting in legal ramifications.
Web application security	Cloud services are typically accessed using web applications. Vulnerabilities in these web applications introduce security risks.
Data breaches	Malicious insiders are a key cause of data breaches. Cloud service provision extends the risk of malicious insiders beyond the enterprise to include cloud service employees.
Virtualisation vulnerability	Control of administrator on host and guest operating systems, imperfect isolation and bugs in virtual machine monitors introduce vulnerabilities.
Availability	Cloud service providers need to ensure plans that offer resilience to hardware/software failures as well as denial of service attacks. Enterprises need to have plans for business continuity and disaster recovery independent of the cloud service provider.
Backup	All data must be backed up for quick recovery and protected to prevent accidental leakage. This may not be a default.

Table 20.3 High-level contractual Issues and challenges in cloud computing agreements (adapted from Leimbach et al., 2014)

Contractual Issue	Challenge
Choice of Law and Legal Jurisdiction	Choice of law may provide advantages to cloud service providers including recognition of disclaimers and limitation of liabilities.
Data Location and Transfer	Transfer of data in-transit or for processing or storage may result in compliance issues or exposure to unanticipated liabilities.
Data Integrity and Availability	Although availability is typically dealt with in the Service Level Agreement, cloud service providers may seek to disclaim liabilities associated with a wide range of causes of unavailability and limit remedies to service credits (based on continued use).
Security of Data	Accommodating discrete security requirements for each client is challenging. As such, agreements are typically standardised and benefit the cloud service provider. Many cloud computing service agreements may not address security for data in-transit, while being processed or in storage.
IP Issues	IP ownership is often not addressed or addressed clearly in cloud service agreements. The ownership in IP in software applications developed by clients should be clearly addressed, particularly where cloud service provider tools are used. Cloud computing service providers are typically exempt of copyright infringement by clients or customers of clients and the Acceptable Use Requirements may allow termination of contract in such cases. Cloud service providers may inadvertently or by intention make use of metadata that contains client data and therefore infringe copyright. Agreements should therefore state clearly what data is being collected by the cloud service provider and for what purpose, and require cloud service providers to warrant against third party patent infringement and indemnify their clients against liabilities associated with such infringements.
Liability and Indemnities	Cloud service providers may attempt to limit direct, indirect and consequential liabilities that may arise from service provision. The extent to which such liabilities and disclaimers are permitted varies across jurisdictions.
Acceptable Use Requirements	There are deterrence mechanisms to protect cloud service providers from the actions of clients or customers of clients. These can be used as the basis for service termination and may contain language unsuitable to the client's customer base thus requiring either disclosure or permission from affected customers.
Service Levels and Performance	Service levels are often standardised, simplistic and designed to protect the cloud service provider not the client. Monitoring of service levels and performance is typically dependent on tools provided by the cloud providers which may have limited transparency on overall performance.
Variation of Contract Terms	Many cloud computing agreements include a reservation of rights to vary the terms of an agreement unilaterally and by reference to changes on a cloud service provider website.