The implementation of SysTrust principles and criteria for assuring reliability of AIS: empirical study

Ahmed H. Al-Dmour and Masam Abood
University of Brunel, London, UK, and

Hani H. Al-Dmour
The University of Jordan, Amman, Jordan

Received 21 May 2017
Revised 26 June 2017
6 July 2017
Accepted 9 July 2017

Abstract

Purpose – This study aims at investigating the extent of SysTrust's framework (principles and criteria) as an internal control approach for assuring the reliability of accounting information system (AIS) were being implemented in Jordanian business organizations.

Design/methodology/approach – The study is based on primary data collected through a structured questionnaire from 239 out of 328 shareholdings companies. The survey units were the shareholding companies in Jordan, and the single key respondents approach was adopted. The extents of SysTrust principles were also measured. Previously validated instruments were used where required. The data were analysed using *t*-test and ANOVA.

Findings – The results indicated that the extent of SysTrust being implemented could be considered to be moderate at this stage. This implies that there are some variations among business organizations in terms of their level of implementing of SysTrust principles and criteria. The results also showed that the extent of SysTrust principles being implemented was varied among business organizations based on their business sector. However, there were not found varied due to their size of business and a length of time in business (experience).

Research limitations/implications – This study is only conducted in Jordan as a developing country. Although Jordan is a valid indicator of prevalent factors in the wider MENA region and developing countries, the lack of external validity of this research means that any generalization of the research findings should be made with caution. Future research can be orientated to other national and cultural settings and compared with the results of this study.

Practical implications – The study provides evidence of the need for management to recognize the importance of the implementation of SysTrust principles and criteria as an internal control for assuring the reliability of AIS within their organizations and be aware which of these principles are appropriate to their size and industry sector.

Originality/value – The findings would be valuable for academic researchers, managers and professional accounting to acquire a better undemanding of the current status of the implementation of the SysTrust principles (i.e., availability, security, integrity processing, confidentiality, and privacy) as an internal control method for assuring the reliability of AIS by testing the phenomenon in Jordan as a developing country.

Keywords Internal control system, AIS, SysTrust principles, Jordanian shareholdings companies

Paper type Research paper

International Journal of Accounting & Information Management
Vol. 27 No. 3, 2019
pp. 461-491
Emerald Publishing Limited
1834-7649
DOI 10.1108/IJAIM-05-2017-0067

Introduction

The adoption of information technology as a pillar in the business world renders it critical in terms of reliability and security. System assurance, as a core part of management, is required to ensure that the accounting system and information initiated is reliable. Information technology in business is essential as long as it is reliable and secure. System reliability in administration primarily guarantees the solidity of data and accounting framework. However, an unreliable system can exhibit a number of side effects, such as failure to prevent unauthorized access to the system, making it vulnerable to viruses, hackers and loss of data confidentiality Loss of data integrity, including defiled, inadequate and invented information, and genuine support issues bringing about unintended negative reactions from system changes, such as loss of access to system administrations, loss of information privacy or loss of information trustworthiness (Boritz, 2005; McPhie, 2000; Topash, 2014). In fact, the complexity of computerized information systems has increased the necessity of the assessment of the reliability of a firm's internal control systems (Joseph *et al.*, 2009).

Furthermore, due to globalization and the advancement of technology around the world, the achievements of the overall objectives of the business become more difficult and complicated. This includes the mission and visions that are also affected by other factors such as fraud, money laundering and terrorism activities. To avoid such challenge caused by advances in technology, companies tend to design their strategies whereby dealing with customers, provision of service, corporate social responsibilities and successful procedure of control system are embedded therein (Douglas, 2011). To enhances and maintain the reliability of control system, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) has developed a new assurance service called SysTrust, whereby a public accountant can write about the adequacy of controls over the reliability of a system. The team formulated a definition of system reliability as "*a system that operates without material error, fault or failure in system availability, privacy, integrity, and maintainability during a specified time in a specified environment*" (Saitio, 2001).

Computerized accounting information systems can face a range of potential threats, and this entails protection of data from abuse and physical and moral loss where administration of business companies tend to design a rigid control system that is reliable and guarantees protection from both internal and external threats. This keeps the quality of outputs of the systems and aids in the efficient achievement of the organization's objectives. Furthermore, a reliable system is also required as continuous auditing is conducted under the supervision of real-time accounting systems. The expected benefits from web-based continuous auditing depend on the reliability of real-time accounting systems. AICPA (2017) pointed out the characteristics of a reliable system as follows:

- *Accuracy*: The system must obtain record and report the information to be audited accurately, completely, and on a timely basis.
- *Security*: There must be controls to prevent unauthorized access to business data and processes. When violations are detected or suspected, the system must warn the auditor and there must be temporary restriction
- *Integrity*: The system processing must be complete, accurate, timely and in accordance with the entity's transaction approval and output distribution policy.
- *Maintainability*: The system must be updated to provide continuous accuracy, security and integrity.

- *Automated auditing programs*: The auditor requires readily made auditing programs or those developed by the auditor because continuous auditing is applied through computing systems.

The core importance of a reliable computing system is specifically identified by the developers of the SysTrust project: *The computing system – are running business, producing products and services and dealing with consumers and business partners [. . .] As business dependencies on information technology increases, tolerance decreases for systems that are unsecured, unenviable when needed, and unable to produce accurate information on an instant basis. Like the weak link in a fence, the unreliable system can cause a chain of events that negatively affect the company and its customers, suppliers and business partners* (ACICPA/CICA, 2013).

In fact, SysTrust acquires its importance because of the following factors:

- It reengineers the internal control system of AIS depending on technological basis.
- It re-conceptualizes AIS-invisible-control-mechanism.
- It enhances standards of operations and security that are designed for increasing efficiency of AIS.
- It grants a guide on a solid ground that helps in measuring AIS reliability and associated risks.

A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. Therefore, any company must have the reliability of the software and database. Romney and Steinbart, (2017), describes the software and databases are not reliable can harm not only the company and employees who use them, but also the company's supply chain.

This study gains its importance as it is represented by that fact that it provides orientation for accounting practitioners, users and auditors who receive better understanding of the implementation of the principles of SysTrust service requirements, and a result, facilitates a more in-depth comprehension and assessment of the applied AIS process in terms of reliability. Furthermore, greater understanding of the empirical literature on accounting information reliability should assist policymakers and regulators in establishing financial reporting standards, auditors to implement standards and financial statement users to evaluate accounting information reliability. A deeper understanding of reliability should also assist academics in conducting research to produce new insights on reliability.

Problem statement

Recently studies have emphasized on the necessity and importance of the internal control system in the accounting information system (Joseph *et al.*, 2009; Al-Laith, 2012; Kuhn *et al.*, 2013). However, articles on SysTrust service engagement as an internal control method for assessing reliability in the professional accounting literature are primarily devoted to explaining the background and purpose of this service and its potential demand (such as in Boritz *et al.*, 1999; Pugliese and Hales, 2000). Furthermore, assessment of the reliability of accounting information system remains under-researched as the majority of such studies have focused on the status of AIS use and its applications (Iceman and Hillson, 2012; Yigitbasioglu, 2016; Tarek *et al.*, 2017). Given that most articles of AIS implementation have been based on cases in Europe and the US, cultural and legislation challenges, although complex, show some inconsistency. However, relatively few studies have been implemented outside of the most developing countries, such as in Jordan, which is a beachhead for new technologies and business practices in the Middle East and North Africa (MENA). Several authors state that within organizations, attention must be given to the accounting standards and laws of each country because they affect accounting management (Davila and Foster, 2005; Tarek *et al.*, 2017; Romney and Steinbart, 2017). Therefore, the purpose of this research is to investigate the extent of the implementation of the SysTrust service framework (principles and criteria) as an internal control method for assessing the reliability of accounting information system processes by Jordanian shareholding companies. The study also aims to examine the whether the level of implementation of SysTrust service framework's requirements are differ on the basis of the demographic characteristics of business organizations (i.e. sector type, size and experience in business).

Research aim, objectives and questions

The research aim is to explore the extent of the implementation of the SysTrust service model's requirements within Jordanian shareholding companies, and to probe the extent to which its main components are implemented and achieved. Specifically, the core objectives of the present study are as follows:

- To identify the extent to which SysTrust model requirements (principles and criteria) for assuring the reliability of the AIS process are implemented or used by the shareholding companies in Jordan. This involves examining the content and context of internal control of AIS in Jordan. Several researchers argue that, within organizations, attention must be given to the accounting standards and laws of each country because they impact on accounting management (Davila and Foster, 2005; Romney and Steinbart, 2017; Tarek *et al.*, 2017).
- To establish any similarities or differences among business companies in respect of the implementation of SysTrust principles and criteria for assuring reliability of AIS process based on their business sector, size and experiences.
- To provide the decision makers with recommendations those aid the account management units in these companies to enhance the reliability of AIS.

The specific questions to be examined are:

Q1. To which extent are the existing AIS processes and applications in the Jordanian shareholding companies reliable in terms of providing the requirements of the five principles of the SysTrust model (availability, security, confidentiality, integrity processing and privacy)?

Q2. Is the level of implementation of SysTrust principles criteria for assuring the reliability of AIS differ according to the demographic characteristics of Jordanian shareholding companies, including sector type, number of employees and business experiences?

Theoretical background and literature review

SysTrust service framework: definition and importance

The SysTrust service framework is an assurance service that was jointly developed by AICPA and CICA. It is designed to increase the comfort of management, customers, and business partners with systems that support a business or particular activity. SysTrust is a type of assurance service performed by a licensed CPA or CA to independently test an organization's system and to offer assurance on the system's reliability. The intent is to enable those who use or rely on the system including the company itself, its partners, and customers to gain trust and confidence in the system (AICPA/CICA, 2017; Bedard *et al.*, 2005). Unlike COCO and COBIT, Trust Services framework was specifically designed for independent auditors to give an audit opinion as to whether the controls around the system were sufficiently effective to deem the system as "reliable". SysTrust initially began as a distinct standard (separate from WebTrust). In 2003, the two standards, SysTrust and WebTrust, were amalgamated into a single standard. However, practitioners can now draw on the relevant principles and criteria from the Trust Services Principles and Criteria framework and give a SysTrust opinion. The standard in its entirety consists of 5 principles, 4 control layers and 139 criteria in total (AICPA/CICA, 2013).

The greatest difference between COBIT and SysTrust can be understood by examining the deliverable that is produced by each framework. COBIT envisions a "maturity model", wherein a firm moves from a low level of maturity (the lowest being 0) to the highest level of maturity. The idea behind assessing the organizations level of maturity is that management will "grade itself" (Martin, 2005). In contrast, SysTrust is designed specifically with the idea that independent auditors will render opinions on the state of control that exists over a system. According to Irving Tyler CIO of Quaker Chemical "COBIT is great from a management point of view, but not all of that applies to Sarbanes-Oxley [. . .] There's lots of good advice and guidance in there that should not be a part of a Sarbanes-Oxley audit" (Martin, 2005). In contrast, the SysTrust framework identifies the specific controls that are necessary to ensure that the system is reliable.

According to the AICPA (2013), SysTrust is an assurance service that independently tests and verifies a system's reliability. The AICPA succinctly describes the overall purpose of SysTrust in the following way: Developments in information technology provide far greater power to companies at far lower costs. As business dependence on information technology increases, tolerance decreases for systems that are not secure, and these systems become unavailable when needed and unable to produce accurate information on a consistent basis. An unreliable system can cause a chain of events that negatively affect a company and its customers, suppliers, and business partners (Boritz and Hunton, 2002). Although COBIT and SysTrust share common foundational frameworks (Committee of Sponsoring Organizations of the Treaway Commission [COSO], 2013), the terminology used to describe information quality is slightly different in each document. Using the definitions contained in each document, the AICPA information qualities have been mapped into the seven COBIT information qualities of efficiency, integrity, effectiveness, availability, confidentiality, reliability and compliance. Five of the COBIT information qualities map directly into the SysTrust principles. Efficiency and reliability are not directly represented (Boritz and Hunton, 2002). An IT control objective is defined by COBIT as "[a] statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity." The objective of a SysTrust engagement is to determine whether management has maintained effective controls over its system to enable the system to function reliably. First, management provides assertions regarding the availability, security, integrity and maintainability of the system. Then, the auditor determines the existence of system controls and performs tests to assess the extent to which such controls were operating effectively during the period covered by the assurance report.

The SysTrust assurance service is distinct from reporting on internal control over financial reporting, which was established in 1993 by the AICPA and is described in SSAE No. 6.5 The latter service is limited to internal controls related to financial reporting and typically uses the criteria established in COSO, *Internal Control: Integrated Framework*. As such, it does not address the reliability of information systems designed for the broader decision needs of management and external users, who may need online access to real-time, updated and accurate information. In contrast, the new SysTrust assurance service relates directly to the overall reliability of a system, regardless of the type of information processed by the system. As such, the system may include financial and nonfinancial information that is critical to management and external users. Martin, (2005) also found the Trust Services framework to be a much more focused framework to work within the context of a SOX engagement and due the Trust Services "focus on the controls that are in place to ensure the company's systems carry out business processes reliably". He also found that the "Trust Services' illustrative controls are detailed enough to help management identify the controls that exist and those that are missing". A reliable system is the one that works without material errors, fault, or failure during a specified time in a specified environment. As for the symptoms of unreliable systems, they include frequent system failures and accidents that prevent users from accessing essential services, failure to prevent unauthorized access to the system, which makes it vulnerable to viruses, hackers and loss of data confidentiality, loss of data integrity, including corrupted, incomplete and fictitious data, and serious maintenance problems resulting in unintended negative side effects (Boritz and Kearns, 2000). This assurance service has the potential to provide a twofold benefit:

(1) enhancing the confidence of a broad audience (management, boards of directors, customers, and business partners) regarding the reliability of information systems (Pugliese and Hales, 2000); and

(2) providing accounting professionals with the ability to leverage their existing skills to fulfil the needs of the systems assurance marketplace (Pugliese and Hales, 2000).

Based on these potential benefits and the increasing dependence of companies on information technology, the profession expects that SysTrust engagements will contribute to the demand for trust services, as well as other assurance services, as predicted by Elliott (1995). Through the WebTrust and SysTrust services, companies have the ability to establish their credibility and build confidence with important end users. SysTrust can benefit a business's day-to-day operations in the following scenarios:

- A company is trying to win a major contract as a supplier to a corporation that uses just-in-time (JIT) inventory management. A SysTrust report that demonstrates the reliability of the company's systems and shows its capacity to be a dependable partner in the JIT environment enables the company to differentiate itself from its competitors.
- A company decides to outsource its human resources, payroll, and other employee-related systems. To ensure smooth operations, it insists that any successful bidder maintain unqualified SysTrust reports on the outsourced systems.
- A retailer qualifies for a discount on business interruption insurance because its SysTrust report attests to the reliability of its inventory management systems.
- When technology problems at foreign subsidiaries cause trouble for an international company, its audit committee decides to adopt the SysTrust principles and criteria as a minimum standard for key subsidiaries (Arnold, *et al.*, 2000).

Users of SysTrust would be interested in a systems assurance examination for some of the following reasons:

- Internal and external users can lose access to essential services because of system failures and crashes.
- Systems can be vulnerable to viruses and hackers because of unauthorized system access.

- System failure can result in loss of access to system services or loss of data confidentiality or integrity.
- Negative publicity in the wake of high-profile system failures can undermine customer and investor confidence.

Regarding the factors and drivers that are behind the demand on this service, (Boritz and Kearns, 2000) pointed out that the demand on this service resulted from companies' search for new markets, reduced costs, and faster change which forced companies to rely on third parties' systems through different ventures. This assurance service profits internal and external parties of the entities that are engaged in information-based commercial activity, such as system users, outsourcing service providers, system developers and consultants, management and board of directors, and internal auditors and system owners (Boritz and Hunton, 2002). Furthermore, as computer systems can be isolated, it is necessary to observe and verify their performance through a capable assurance provider, and also as an IT is a complex field, it requires special expertise. System unreliability can pose a risk due to making incorrect decisions for system users, or when there are major consequences related to unreliability, such as unnecessary costs, poor revenue, loss of investors' trust due to system failure; therefore, assurance on system reliability is greatly valued (Boritz and Hunton, 2002; El-Syaed and Hassan, 2010). Boritz *et al.* (1999) and McPhie (2000) have documented several examples of unreliable systems. These include:

- denial of service, where users cannot use the system because it fails or crashes, or there are capacity issues;
- unauthorized access, where the system is working, but viruses or hackers invade the system, or confidentiality is lost; and
- loss of data integrity, where information is corrupted, incomplete or fictitious.

In a SysTrust service, the management of a company prepares a description that defines the aspects of the system that will be covered, so that the scope is clear to users of the report. Then, a licensed practitioner (CPA or CA) performs audit procedures to examine and test the five key components of the system (infrastructure, software, people, procedures, and data), as well as their relationships. Finally, the practitioner assesses whether the whole system meets the SysTrust principles and the related criteria. If the system satisfactorily meets all the principles and the related criteria, it achieves the reliability defined by SysTrust. The practitioner will issue a written SysTrust assurance report with an unqualified opinion, independently verifying that the company has effective system controls and safeguards enabling the system to function reliably. The company may use the SysTrust assurance report in its marketing of documents, agreements and contract with customers, business partners or others system users to enhance trust in its system. Concerning the participating parties in the assurance services, Bedard *et al.* (2005) notes that there are three parties involved in systems assurance services:

- the users of the assurance services;
- the entity hiring the assuror (assurance provider); and
- the assuror or "provider".

Assurance providers play a crucial role in the assurance service engagement, and they should have certain attributes. Knechel *et al.* (2006) discusses the required attributes of assurance service providers by using a sample of Dutch senior accounting and financial officers, and suggests certain attributes: confidentiality, expertise, professional reputation, independence, objectivity, integrity, and costliness. They concluded that overall expertise and objectivity are perceived to be the most important attributes for selecting an assurance service provider. Cost is perceived as the least important attribute for assurance services in general. Most respondents (97.6 per cent) agree that expertise is important in the assessment of systems reliability. In addition, the provider of system trust service should have skills related to information technology; however, the degree of complexity depends on the system being examined (Boritz *et al.*, 1999).

The AICPA (2013) Assurance Services Executive Committee has developed a set of principles and criteria (trust services principles and criteria) to be used in evaluating controls relevant to the security, availability, and integrity processing of a system, and the confidentiality and privacy of the information processed by the system. In this document, a *system* is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management specified requirements. System components can be classified into the following five categories:

(1) *Infrastructure*: The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices and telecommunications networks).

(2) *Software*: The application programs and IT system software that supports application programs (operating systems, middleware and utilities).

(3) *People*: The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel and managers).

(4) *Processes*: The automated and manual procedures.

(5) *Data*. The information used or processed by a system (transaction streams, files, databases and tables).

The AICPA (2013) and CICA have developed the following principles and related criteria for use by practitioners in the performance of trust services engagements.

Availability. The system is available for operation and use as committed or agreed. The *availability principle* refers to access to the system, products, or services that contract, service-level, or other agreements advertise or agree. To note, the principle itself does not set a minimum acceptable performance level for system availability. The minimum performance level is confirmed through a mutual agreement (contract) agreed upon between parties. The *availability principle* does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance. In assuring availability, the SysTrust provider attests that accessibility to the system, products or services is available as committed to, or agreed upon, by the entity.

Security. The *security principle* refers to the protection of the system resources through logical and physical access control measures to support the achievement of management's commitments and requirements related to security, availability, integrity processing, and confidentiality. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information. Assurance of system security implies that access is restricted to the physical components of the system, the logical functions the system performs, and the information stored in the system (AICPA, 2013).

Processing integrity. The *integrity processing principle* refers to the completeness, accuracy, validity, timeliness, and authorization of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Completeness generally indicates that all transactions are processed or all services are performed without exception. Validity refers to processing transactions and services no more than once and with compliance to business principles and expectations. Accuracy refers to keeping important information, concerning the submitted transaction, accurate while the transaction is being processed and that the transaction or service is processed as planned. The agreement context made for the provision of services or delivery of goods shows their eligibility (AICPA, 2013, 2017). Authorization means that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, accurate, current, and authorized. System control usually cannot address the risk that data contain errors introduced prior to its input in the system, and the unit is not usually liable to identify these types of errors. In the same way, users from outside the system boundary may be accountable for starting processing. The data may become invalid, imprecise, or unsuitable if actions such as these are not taken. System integrity processing refers to the completeness, accuracy, timeliness, and authorization of system processing (i.e., all phases of processing, including input, transmission, processing, storage, and output). If integrity processing is not present, even a system that is secure and available is of little benefit to users. While the number of audit failures directly attributed to inaccurate assessment of controls is relatively small, there have been a significant number of system failures that have caused users untold grief. System integrity processing addresses all system components and all phases of processing (input, transmission, processing, storage, and output) that are the subject of the SysTrust engagement. If a system processes information inputs from sources outside the system's boundaries, an entity can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing because, for the most part, procedures at external sites are beyond the entity's control. Thus, when the information source is explicitly excluded from the boundaries of the system that define the SysTrust engagement, it is important to describe that exclusion in the system description. In other cases, the data source may be an inherent part of the system being examined, and controls over the completeness, accuracy, authorization, and timeliness of information submitted for processing would be included in the system description (ACIPA, 2017).

System integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation of the system. In this document, system integrity refers to the completeness, accuracy, timeliness, and authorization of system processing. In this document, data integrity refers to the completeness, accuracy, currency, and authorization of data. Data integrity depends on system integrity, and system integrity depends on controls over system components and the risks affecting those components in the system's business context. Although system and data integrity are obviously related, the focus of a SysTrust engagement is system integrity. Because SysTrust is a controls-based engagement, ordinarily it would not provide sufficient evidence to enable a practitioner to provide examination level assurance about data integrity (AICPA, 2013). This is due to the following inherent limitations of controls:

- the possibility of circumvention, either by employee collusion or management override, when it is difficult to prevent or detect such circumvention;

- the trade-off between operating efficiency and complex controls that may reduce exposure;
- the practical materiality limits, below which it is impractical to implement controls;
- changing conditions in entities that may lead controls to deteriorate or to become inappropriate; and
- the reliance on human judgment in the design, implementation, and monitoring of controls, any of which may lead to control breakdowns.

Because of the inherent limitations of controls, evidence about the effectiveness of controls over system integrity ordinarily would not provide sufficient evidence about data integrity to reduce attestation risk to the low level required. Thus, although evidence about the effectiveness of controls over system integrity may be very persuasive, procedures beyond those performed in a SysTrust examination would be required to reduce attestation risk about data integrity to a level required by examination-level attestation standards. It is also important to recognize that system integrity does not automatically imply that the information stored by the system is complete, accurate, current, and authorized. This is because errors may have been introduced into system data at some previous time (for example, at initial data conversion) and those errors could still be present in the data, even though current system processing may be complete, accurate, timely, and authorized.

Confidentiality

The confidentiality principle refers to the system's ability to protect the information designated as confidential, as committed or agreed. Unlike personal information, which is defined by regulation in a number of countries worldwide and is subject to the privacy principles, there is no widely reorganized definition of what constitutes confidential information (AICPA, 2006, 2013). Partners usually exchange information that need to be kept confidential, at the time of communicating and transacting business. Often the request of respective parties is that they be assured that the information they give is only accessible for those individuals who need access to it, to complete the transaction or to clarify any questions that may arise. To enhance business partner confidence, it is important that the business partner be informed about the entity's system and information confidentiality policies, procedures, and practices. The entity needs to disclose its system and information confidentiality policies, procedures, and practices relating to the manner in which it provides for an authorized access to its system, and uses and shares information designated as confidential. The need for information to be confidential may arise for many different reasons. For example, the information is proprietary information, information intended only for company personnel, personal information, or merely embarrassing information. Confidentiality is distinguished from privacy, in that:

- Privacy deals with personal information, whereas confidentiality refers to a broader range of information that is not restricted to personal information.
- Privacy addresses requirements for the treatment, processing, and handling of personal information (AICPA, 2013, 2017).

Privacy. Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information. Distributed by the AICPA and CICA, criteria set forth in Generally Accepted Privacy Principles indicate that personal information is collected, used, maintained, disclosed, and destroyed. This is also in compliance with the agreements in the entity's privacy notice. *Personal Information* refers to information relative to an identifiable individual and includes any information that can be directly or indirectly used to identify an individual, and any information that can be connected to an individual. Any information, gathered by an organization, which can be linked to an individual, is most often considered personal information. Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, all businesses need to effectively address privacy as a risk management issue. The following are specific risks of having inadequate privacy policies and procedures (AICPA, 2013):

- damage to the organization's reputation, brand or business relationships;
- legal liability and industry or regulatory sanctions;
- charges of deceptive business practices;
- customer or employee distrust;
- denial of consent by individuals to have their personal information used for business purposes;
- lost business and consequential reduction in revenue and market share;
- disruption of international business operations; and
- liability resulting from identity theft.

For organizations operating in more than one country, the management of their privacy risk can be a significant challenge. For example, the global nature of the Internet and business means regulatory actions in one country may affect the rights and obligations of individual users and customers around the world. Many countries have laws regulating trans-border data flow, including the European Union's (EU) directives on data protection and privacy, with which an organization must comply if it wants to do business in those countries *(*AICPA, 2013). Therefore, organizations need to comply with changing privacy requirements around the world. Further, different jurisdictions have different privacy philosophies, making international compliance a complex task. To illustrate this, some countries view personal information as belonging to the individual and take the position that the enterprise has a fiduciary-like relationship when collecting and maintaining such information. Alternatively, other countries view personal information as belonging to the enterprise that collects it. In addition, organizations are challenged to try and stay up-to-date with the requirements for each country in which they do business. By adhering to a high global standard, such as those set out in this document, compliance with many regulations will be facilitated. Even organizations with limited international exposure often face issues of compliance with privacy requirements in other countries. Many of these organizations are unsure how to address often stricter overseas regulations. This increases the risk that an organization inadvertently could commit a breach that becomes an example to be publicized by the offended host country. Furthermore, many local jurisdictions (such as states or provinces) and certain industries, such as healthcare or banking, have specific requirements related to privacy. The trust services framework identifies four essential criteria for successfully implementing each of the five principles that contribute to systems reliability (AICPA, 2013):

(1) *Developing and documenting policies*. The entity has defined and documented its policies relevant to the particular principle. (The term *policies* as used here refer to written statements that communicate management's intent, objectives, requirements, responsibilities, and standards for a particular subject.)

Management needs to develop a comprehensive set of security polices before designing and implementing specific control procedures. Developing a comprehensive set of security policies begins by taking an inventory of information system resources. This includes not only hardware but also software and database.

(2) *Effectively communicating policies to all authorized users.* The entity has communicated its defined policies to responsible parties and authorized users of the system. To be effective, this communication must involve more than just handling people written documents and asking them to sign an acknowledgment that they received and read them. Instead, users must receive regular, periodic reminders about security and training in how to use them.

(3) *Designing and employing appropriate control procedures to implement.* The entity placed in operation procedures to achieve its objectives in accordance with its defined policies.

(4) *Monitoring the system and taking a corrective action to maintain compliance with policies*: The entity monitors the system and takes action to maintain compliance with its defined policies. Effective control system involves a continuous cycle of developing policies to address identified threats, communicating those policies to all employees, implementing specific control procedures to mitigate risks, monitoring performance and taking a corrective action in response to identified problems. The necessary corrective action often involves the modification of the existing policies and the development of new ones.

Literature review

To survey empirical studies pertinent to the reliability of AIS as the main focus, a scholarly internet search engine (scholar.google.com), in addition to several online databases, was used. The databases cover all leading journals, not only in the fields of internal control of AIS process, but also in the accounting of information systems in general and the recently developing field of trust service in e-commerce and accounting. AIS is embedded within IS journals. The majority are conceptual or non-empirical, where the empirical previous studies that discuss the same topic apply one of the two approaches, either qualitative or quantitative. The theory of demand for trust services is based on some innate hardships related to electronic commerce. While all business transactions carry a risk factor that intended transactions will not be processed as planned, the risk factor is greater in electronic commerce because of the loss of human mediators that are at hand in physical markets, indicating a reliance on electronic systems to avert, or identify and correct, errors (Tan and Theon, 2002). In addition, as information irregularity between parties to transactions is higher in electronic commerce, they are usually geologically distributed (Enofe *et al.*, 2012; Al-Laith, 2012).

Henry (1997) carries out a survey on 261 companies in the USA to determine the nature of their accounting systems and security in use. Seven basic security methods were presented in his study. These methods were encryption, password access, backup of the data, viruses' protection, and authorization for system changes, physical system security and periodic audit. Henry's study results indicate that 80.3 per cent of the companies' backup their accounting systems, 74.4 per cent of the companies secure their accounting systems with passwords, where only 42.7 per cent use antivirus in their systems. The results also reveal that less than 6 per cent of the companies use data encryption, lastly 45 per cent of companies undergo some sort of periodic audit for their accounting information systems. Another study, carried out by Qurashi and Siegel (1997), assures the accountant's responsibility to check the security of the computer system. The researchers carried out a theoretical study to develop a security checklist. This list covers the following four security controls groups: Client policy, Software security, Hardware security and Data security. Cerullo and Michael (1999) conducted a survey using a questionnaire of twenty potential security and control mechanisms, which was circulated among audit directors of two hundred fortune companies in the USA. These mechanisms were placed by Cerullo study in four categories, namely, client-, network-, server- and application-based. Tan and Theon (2002) conclude that parties would not use an electronic transaction unless the degree of transaction trust is higher than the threshold value, which relies on features of the party and of the transaction itself. The possibility to resist taking part in electronic transactions develops the requirement for a service that will strengthen trust to the level that it exceeds the user's threshold.

WebTrust and SysTrust deal with this requirement through assuring observance of standards of control. Together, the attributes of the particular assurances made (e.g. reliability, privacy, etc.), and the attributes of the assuring party (Kaplan and Nieschwietz, 2003) are theorized to result in the trust-enhancing value of these services. From amongst trust services literature, the researchers Kovar and Mauldin (2003) give a theoretical model that targets its focus on the natural prospective need for assurance services, resulting together from circumstantial business setting features and sources of information risk within that setting and from a precedent of the market demand for third-party assurance services. Furthermore, many studies investigate whether web trust influence consumers' concerns about taking part in online transactions (McCole, *et al.*, 2010; Fortesa and Ritab, 2016). These studies tend to find a positive influence of WebTrust on customers' attitudes and/or behaviour, but also find that the level of the influence varies according to the knowledge of the customers, which includes their familiarity with the service.

Additionally, Arnold *et al.* (2000) find that a graded report may be more informative than the binary report that is presently administered (i.e. reporting that the service either meets or does not meet certain criteria). Also, experimental studies tend to find that the effect of WebTrust is similar to that of other competitive products, signifying consumers' lack of ability to differentiate between them. Findings from other research reveal that as well as consumers, financial professionals may also help WebTrust in the decisions they make. Hunton *et al.* (2000) find that WebTrust assurance results in greater earnings forecasts and stock price estimates by financial researchers, indicating conviction that a WebTrust seal is related to greater quality and, therefore, better expectations for future business. Because SysTrust was created after WebTrust, there is a lack of experimental research available in that perspective. In their study of electronic data interchange (EDI), Khazanchi and Sutton (2001) give evidence of the requirement for systems assurance, illustrating that numerous companies enforcing these systems do not use them to full benefit. This shows that entities authorizing EDI for their clients or customers should require assurance of suitable functioning. Results of these studies recommend a demand for trust services. Consequently, it follows that there should be a positive effect on the business of clients that meet approved trust services standards. Moreover, a study from Havelka *et al.* (1998) argues that expression of agreement on measurement criteria for assurance services among providers and users will enable a more effective and efficient production of those services.

They created measurement criteria for assurance services generally, and made a comparison of the views of IT consultants and system users on the related significance of those criteria in performing systems assurance. While current research indicates that trust services assist in reducing user resistance to depend on companies' systems when undertaking electronic commerce, many types of possible future research appear from methodological and theoretical issues concerning the existing standing of the literature in this area. One methodological concern emerges from the knowledge that the prime research method used is the behavioural experiment. Experimental methods are important because they are strong in internal validity. However, if there were archival research and field studies in addition to behavioural research, understanding of users' demand for trust services and the impact on user decisions would be improved. As written in the financial statement auditing literature, targeting research on actual users' experiences would allow a stability of internal and external validity. For example, experimental research could be important in evaluating the nature of demand for trust services. The principal theories available regarding user demand are connected to the presence of threshold levels of trust needed to decrease resistance in using electronic commerce. In hypothetical scenarios, usually found in behavioural experiments, it may be hard to imitate this resistance. Information not available on the difference on how users' threshold trust levels, and factors connected with this variance, make it difficult to explain demand for trust services in general and for the particular aspects of these services in particular. Another theoretical issue is that so far there has been no research that addresses users' assumptions regarding outcomes of trust services, or what their actions would be if these assumptions are not met. Supposedly, if an assurance services' trust levels increased to the level that a formerly resistant party uses electronic commerce, then that user will uphold the assumption that trade will continue in a safe and continuous way. Breach of this assumption could result in legal actions against the provider because this issue is related to verification risk for the assuror and is explained in the provider's section below.

Chang's (2001) research declares that organizational effectiveness in a worldwide competitive environment is extensively attributed to accounting information. Doms *et al.* (2004) point out that the most significant source of externally viable information on companies is still financial statements. There is some concern that accounting practice is not up-to-date with fast economic and high technology changes, in spite of their widespread use and continuing advance, which consistently affects the significance value of accounting information. The significance of Chang's declaration is strengthened by a fast changing business environment and reports by some researchers indicating that the importance value of accounting information has decreased due to an increase in accounting fraud in developed countries such as the USA. Furthermore, SysTrust is one of the models to update Internal Control Systems (ICS) of AIS through frame working the technological variables which affect designing AIS. Due to such nature, much of the practical studies have been implemented using the principles and criteria of SysTrust to examine quality and performance of AIS. The term ICS has been used by COSO (2013) to refer to the risks associated with ineffectiveness management of public companies, both large and small. Integrated framework of COSO has long served as a blueprint for establishing internal controls that promote efficiency, minimize risks, help check the reliability of financial statements, and comply with laws and regulations. According to COSO's study, ICS is no longer accounting concept. COSO's report has outlined 26 fundamental principles associated with the five key components of ICS: control environment, risk assessment, control activities, information and communication and monitoring. SACF (2001) considers the control objectives associated with use of IT. The study is widely known as COBIT. COBIT consists of three control groups: business objectives, IT resources, and IT-based process. The key feature of COBIT is coming from the fact that it has developed 36 standards of control related to security of IT-based AIS. The impact of IT formed an accounting process on the operational variables of cost and productivity, and profitability has been addressed by Casolaro and Gobbi (2004). The study was conducted on more than 600 banks belonging to the Italian banking industry. The study concludes with the facts that intensive use of IT-based AIS has reasonable impact on:

- reduction of banking services cost,
- expansion of banking services package, and
- increasing banking profit.

Another study was conducted by Raupeliene and Stabingis, (2003) has considered the effectiveness of IT based AIS. The study has developed a quantitative model based on set of technological, economics, and social parameters. Their study revealed that the effectiveness of IT-based AIS varies according to the superiority level of IT infrastructure of AIS and the environmental development of AIS.

A study by Warren (2002) entitled "Security Practices" attempts to study the difficulties facing the information system using a sample consisting of Australian, English and American companies. The results of the study show that the limitation of technological security procedures and intentional incorrect entry of financial data in the American companies is a noticeable limitation facing information system. Previous literature discussed the effect of assurance on its beneficiaries. Boritz and Hunton (2002) tried to evaluate the amount that auditor-provided systems reliability assurance affects prospective service recipients' through

- the probability of recommending that their company enter into a contractual agreement with the service provider, and
- the comfort level with the reliability of the service provider's information systems.

Abu Musa (2004) performs an empirical study to investigate the adequacy of security controls implemented in the Egyptian banking industry (EBI), where the respondents were limited to the head of the computer department and the head of internal audit department. Abu Musa tried to check whether the applied Security Controls in the EBI are adequate to protect against the perceived security threats through self-administrated checklist. The CAIS security checklist included eighty security procedures which were categorized under the following ten groups.

(1) Organizational information security controls.
(2) Hardware and physical access security controls.
(3) Software and electronic access security controls.
(4) Data and data integrity security controls.
(5) Off-line programs and data security controls.
(6) Utility security Controls.
(7) Bypassing of normal access security controls.
(8) User programming security controls.
(9) Division of duties.
(10) Output security control.

Another empirical study was conducted by Abu-Musa (2010) in Saudi Arabia, shows that the majority of business organizations not have disaster recovery plans to deal with information security incidents and emergencies as well as information security functions and authorities are not well–identified and communicated. In addition, it also indicates that the risk assessment process and procedures are not appropriately and effectively executed.

Boritz (2005) conducts an extensive review of the literature to identify the key attributes of information integrity and related issues. He brought two focus groups of experienced practitioners to discuss the documented findings extracted from the literature review through questionnaire examining the core concepts of information integrity and it elements. He considers information security as one of the core attributes for information integrity. This security should cover the following areas: physical access controls and logical access controls. The results indicate that the security has a lower impairment severity score than other severe practical aspects, such as availability and verifiability. Boritz's such findings refer to the effective use of security controls in the organizations represented.

In his study, Martin (2005) focuses on the fulfilment of Sarbanes-Oxley act 2002 that requires public companies to report about the effectiveness of their internal control systems He explained that the American companies are using COBIT for Sarbanes-Oxley act 2002 compliance, and this is because its objectives have been mapped to COSO in a publication entitled IT Control Objectives for Sarbanes-Oxley. COBIT also has been mapped to popular enterprise resource planning (ERP) systems, such as SAP, Oracle and PeopleSoft. This mapping and related guidance provides COBIT with framework references and methodologies for auditing and testing the major ERP systems. But it is decided later to use SysTrust service to ensure the company's systems carry-out business processes reliably. Herein, Martin establishes five-step processes showing how the CPAs can use the trust service framework to evaluate a company's IT controls when the entity primarily uses the COSO approach. These steps are:

- Use COSO framework to identify the risks in each business cycle and the controls that mitigate them,
- Gather initial IT information,
- Identify all information systems that relate to financial reporting.
- Be used to trust services framework to create one overall IT matrix,
- Assess the controls identified in the matrixes created above.

Martin (2005) mentions the same steps in his study, in which he tries to explain how information system auditor can use the AICPA/CICA trust services framework to evaluate internal controls, particularly controls over information technology. The participants in the experiment were 481 middle and upper-level managers from a wide range of functional areas. The study concludes that auditor-provided assurances on information systems availability security, integrity and maintainability will show significant key effects with respect to the probability of the participant entering into a contractual agreement with the ASP organization. In addition, the comfort level of the participant with the reliability of the ASP organization's ERP system will increase.

In the same perspective, Mauldin *et al.* (2006) investigate the possible demand for third-party assurance reports in business-to-business electronic commerce (B2B e-commerce) by observing the purchase decisions of 95 professionals to advise using a B2B exchange. The experiment uses the 2 × 2 between subject's design, and varies the assurance scope (system related assurance vs. data related assurance) and assurance timing (continuous assurance vs static assurance) with another control condition of no assurance. The results of the study show that there is more probability of purchasing professionals advising using the exchange when general assurance over the reliability of the exchange's system exists, than when specific assurance over the reliability of transaction information exists. There is also a greater chance of purchasing professionals advising using the exchange when the assurance report is continuous than when it is static, issued at a given time. However, the results also suggest that those participating are less probable to recommend using the exchange when specific information assurance or static assurance exists than when assurance does not exist at all. Also, Meharia (2012) aims to study the effects of assurance services and the trust in the mobile payment system on how users' use the system. To demonstrate this matter, the study depends on the Technology Acceptance Model (TAM). The study finds that the users' intention to use their attitude towards the system determines their real use. Their attitude towards the system is decided by the apparent usefulness of the system and the simplicity of use. However, the study adds that the assurance on the security, availability, confidentiality, privacy, and process integrity of the system will have a positive influence on the users' attitude towards the system, in combination with the apparent usefulness and simplicity of use.

Also, from a security perspective, Siponen and Oinas-Kukkonen (2007) reconcile prior security research literature and emphasize the distinct importance of accessibility and availability as it relates to communication issues, like user authentication and appropriate maintenance of data retention. Strong *et al.* (1997) also segregate and highlight the importance of accessibility as a determinant of data quality. In particular, they emphasize the importance of access security and timely availability to data. Likewise, Nelson *et al.* (2005) argue that accessibility represents a system attribute that is distinct but similar in importance to the system's ability to produce reliable data, although they argue that this impact of accessibility is second in order of influence to the system's processing reliability. In the same manner, Zhou (2011) intends to evaluate the influence of initial trust on user adoption of mobile banking. The study supposes that initial trust decides the intent to use the mobile banking system, as well as the apparent usefulness of the system. The initial trust is decided by the structural assurance (such as third party certifications), information quality, and system quality. The apparent usefulness is decided by the information quality and system quality. Information quality indicates the relevance, adequacy, precision and timeliness of the information. Whereas system quality indicates the speed of access, simplicity of use, navigation and look of the mobile banking system (Kim *et al.*, 2004 as cited in Zhou, 2011). The study finds that structural assurance, information quality, and system quality have an influence on initial trust. Users need to depend on structural assurance to trust mobile banking because mobile banking relies on wireless networks and includes great risk and doubt. Information quality and system quality have an influence on the apparent usefulness of the mobile banking system. Users may feel that the providers of these types of system will not provide quality services to them if the quality of information is low.

Furthermore, if mobile banking has a slow access speed or if users experience service unavailability or interruption, because of system unreliability, users' observation towards mobile banking will have a negative effect. In the same context, Greenberg *et al.* (2012) aim to investigate the influence of SysTrust criteria (availability, integrity and security) on users' intent to use reliability on an online accounting system (of Oracle Small Business Suite). According to the TAM, the study supposes that the intention to take up online systems depends on the apparent usefulness of the system, apparent ease of use, trust in system reliability, and trust in the internet. The study finds that users' intention to take up the online accounting system is greater when users' trust in system reliability and trust in the internet are greater. The results of the study indicate that the reliability of a system, as measured by SysTrust criteria, is related to the decisions relevant to the intention to take up online accounting systems. Consequently, it is apparent that system assurance has a positive influence on system users, their reliance and, therefore, on their decisions, particularly when this assurance is provided constantly, which is more suitable according to the present changing environment. The study by Topash (2014) likewise found that the accompanying criteria or indicators should be available in any accounting information system for it to be productive in any organization which is, cost effectiveness, great documentation, presence of legitimate safety efforts, free inward and outside review, separation of other operation from accounting, and effective internal control. In smellier vain, Daneila (2013), state that accounting information systems and internal controls have a positive relationship to the financial reporting to produce reliable financial statements.

In reviewing the literature, it can be seen that Certified Public Accountants (CPAs) can provide assurance on RTA Information Systems. CPAs are accepted as independent parties that provide assurance concerning the accuracy and fairness of financial information (Boritz and Hunton, 2002), CPA, also acquire advanced technical competencies (Burton, *et al*., 2012). Boritz and Hunton (2002) aim to assess the extent to which auditor-provided systems reliability assurance affects potential service recipients':

1. likelihood of recommending that their company should enter into a contractual agreement with the service provider; and
2. comfort level with the reliability of the service provider's information systems.

Based on an experiment on 481 middle- and upper-level managers from a broad spectrum of functional areas participating in the study, the conclusion is that auditor-provided assurances on information systems availability security, integrity and maintainability will exhibit significant main effects with respect to the participants' likelihood of entering into a contractual agreement with the ASP firm and the participants' comfort level with the reliability of the ASP firm's ERP system will increase. Similarly, Greenberg *et al.* (2012) have attempted to study the impact of SysTrust criteria on users' intention to use online accounting systems and their reliability. Based on the TAM, the study posits that the intention to adopt online systems depend on the perceived usefulness of the system, perceived ease of use, trust in system reliability, and trust in the internet. The study finds that users' intention to adopt the online accounting system is higher when users' trust in system reliability and trust in the internet are higher. The results of the study suggest that the reliability of a system, as measured by SysTrust criteria, is relevant to the decisions related to the intention to adopt online accounting systems.

Furthermore, it is predicted that accounting organizations will benefit from their long experience of financial audits and will probably surpass other types of assurance providers in the formal application of non-financial assurance services (Perego, 2009). Additionally, when providing financial matters, CPAs should follow strict and comprehensive ethical and professional standards (Boritz and Hunton, 2002). For this reason, the American Institute of Certified Public Accountants (AICPA) considers assurance service on electronic systems a logical and natural extension to the already present services that the auditor provides (AICPA, 2017). Proposed benefits of the use of SysTrust service include improved confidence in the systems of both business partners' and one's own internal systems, avoiding problems of system development (McPhie, 2000) and reducing the cost of business interruption insurance (Pugliese and Hales, 2000). The literature also suggests that SysTrust provides a good framework for auditing internal systems and restructuring systems controls and procedures (Bedard *et al.*, 2005). It also sets a standard for structuring information technology outsourcing agreements. While recognizing the potential benefits of trust services, Gray (2002) warns customers to investigate the relative value of the benefits against the associated cost before hiring a third party assurance provider. Accordingly, it is clear that system assurance has a positive impact on system users and their reliance and in turn on their decisions, especially when this assurance is provided on continuous basis, which is more suitable to the current changing environment. SysTrust developers also expect that the SysTrust report would be seen in the market as a sign of quality. According to this viewpoint, Bedard *et al.* (2005) imply that SysTrust opinions will function as a marketing tool and add value for the client. In the most recent version of the trust services guidelines, electronic seals or reports can be used with SysTrust engagements. Users may recognize that displaying the electronic seals or reports will help in their marketing efforts through improving their skill to distinguish themselves from other entities. This contention is supported by the results of the study of Arnold *et al.* (2000), which indicate that good-quality dealers are willing to pay for reports that differentiate along quality lines.

Moreover, Boritz and Hunton (2002) report that SysTrust assurance significantly increases user comfort levels with the reliability of the information technology of a service provider, as well as the possibility that users would recommend contracting with the service providers. Even though the possible benefits of trust services to clients have been focused on in the literature, there is a lack of experimental evidence to support the belief that the existence of a trust service assurance report gives a precise sign of systems quality. The study by Jamal and Maier (2002) focuses on this aspect and examines the link between the existence of web seals and actual company practices with regard to information privacy. The results indicate that, on overall, clients comply reasonably well with privacy policies concerning notification, disclosure, and privately identifiable information choice options. While compliance with acknowledged privacy policies is not perfect, Jamal and Maier (2002) find that disclosure for web sites with privacy seals is better than those without seals. Enofe *et al.* (2012) Amin and Mohamed, (2016), also indicated that an accounting process and continuous auditing cannot be conducted effectively in today worldwide market without the use of computer and accounting software. They believed that changes in the accounting profession are the main reason behind the necessity of internal control accounting system to increase security and protection. However, performing SysTrust engagements is not without potential risks. There are two potential issues inherent in such engagements, some of which present exposures to the provider of assurance services. For example, users might not recognize that trust services cannot provide continuous assurance regarding system, and further performance might not be predictable based on past performance and test (Bedard, *et al.*, 2005).

Experimental work indicates that there would be demand for both WebTrust (Hunton *et al.*, 2000; Arens *et al.*, 2014 and SysTrust (Boritz and Hunton, 2002; Arens *et al.*, 2014) in the marketplace. Yet, as Bedard *et al.* (2005) note, there are a lot of issues, questions and risks in SysTrust engagements, and most auditors are leery about delving into the ill-defined arena of systems reliability assurance. Only limited research to date has looked at ways in which to improve and deliver systems reliability assurance. Havelka *et al.* (1998) conduct a series of focus groups with systems development teams to establish criteria for assessing the quality of the information. Arnold *et al.* (2000) explore the market demand for graded reporting of systems quality versus use of a traditional auditor's binary reporting model. These studies represent the first incremental steps in understanding systems reliability assurance. The domain is wide, open, and in great need of additional research. While SysTrust provides some broad criteria that must be considered in assessing systems reliability, little is known about how to go about assessing these criteria effectively. Given the major role that IT systems play, particularly in enterprise systems environments, the profession must rapidly advance its ability to assess systems quality and academic researchers need to step forward in helping answer the difficult questions that to date present barriers to widespread systems reliability assurance efforts.

After reviewing the previous studies, in this specific area of research, relating to reliability and of the evaluation of CAIS control systems, it can be observed that there are not enough empirical studies available, and this could be due to the fact that this area of research is reasonably new. In addition, many of the studies in this subject are administered on a small level and connected with combined studies from the fields of business management, computer science, and at times engineering. They are often in the form of reports or descriptive studies, and rarely experimental. Furthermore, studies on SysTrust service engagement as an internal control method for assessing reliability in the professional accounting literature are primarily devoted to explaining the background and purpose of this service and its potential demand (Boritz and Kearns, 2000; Pugliese and Hales, 2000; Tarek *et al.*, 2017). Related empirical research also primarily addresses topics related to user demand for trust services. In addition, there has been relatively little business-oriented research on reliability. It should also be noted that some of the investigations are conducted in isolation, without benefit from the experience of findings from other studies. It should also be noted that the majority of these studies are confined to the experience of developed countries, such as in Europe and the USA. It is observed that in many of these studies, practical implications of research findings are only stated in general terms, and little attempt has been made to report the reliability of the scales of measurement used for data collection. Given that most studies of AIS implementation have been based on cases in Europe and the US, cultural and legislation challenges, although complex, show some consistency. However, relatively few studies have been investigated outside of the most developed countries, such as in Jordan, which is a beachhead for new technologies and business practices in the Middle East and North Africa (MENA). Several authors state that within organizations, there must be attention given to the accounting standards and laws of each country, because they affect accounting management (Davila and Foster, 2005; Romney and Steinbart, 2017).

Research hypotheses

Based upon theoretical background and literature review, the following hypotheses are examined in this study**:**

H1. The SysTrust principles and criteria (i.e. five principles: availability, security, integrity data processing, confidentiality, and privacy) are not significantly implemented in the business organizations.

H2. There is no significant difference among business organizations in terms of the extent of SysTrust principles and criteria being implemented based on their type of business sector.

H3. There is no significant difference among business organizations in terms of the extent of SysTrust principles and criteria a being implemented based on their size of business.

H4. There is no significant difference among business organizations in terms of the extent of extent of SysTrust principles and criteria being implemented based on their business experience.

Research methodology

The data for this research were collected through self –administrated questionnaire. The target respondents were all the shareholding companies in Jordan and the single key respondents approach was used. The key respondent was financial/account manager/

director. The identification of the individual business organizations in the country (Jordan) could be done by obtaining names of all companies, as well as their addresses, from a variety of private and public sources to identify the type of business sector, and the range of the number of companies in each sector. Restrictions of time and financial resources could make the inclusion of all business companies impossible. Therefore, the target population is only limited to all shareholding companies listed in Amman Stock Exchange Market database in 2016. Table I demonstrates the demographic characteristics of the study's population. A total of 328 self-administrated questionnaires were distributed to the respondents by e-mail and hand and the response rate was 73 per cent. 68 per cent of the respondents were from service sector. Initially, research assistants called the companies to have appointments to distribute copies of the questionnaire to their companies. After respondents answered the questions, the assistants collected the copies from them.

In this survey, some variables are factual (for example, companies' demographic characteristics such as the type of sector, business experience and number of employees), whereas others are perceptual (i.e. SysTrust principles and criteria). The extent of the implementation of SysTrust principles and criteria were measured using a seven–point Likert scale with anchor ranging from (1) "not implemented at all" to (7) "highly implemented"). The study is based on primary data and the time period is cross-sectional. For data collection, a structured questionnaire was developed and collected data were fed to the statistical software called SPSS-20 to analyse. Simple statistical tools like, mean, standard deviation, and ANOVA were applied. The questionnaire's content (constructs and measures) were mainly selected from AICPA (2013) framework and some previous studies and were modified to the practice of Jordanian shareholding companies' context based on the results of a pilot study and feedback from five professional academic staff in this filed. Table II shows five fundamental principles and criteria and related measures that used in the study.

Data analysis

Reliability

As shown in Table III, all principles of SysTrust were tested to ensure an adequate level of scales reliability using Cronbach's alpha, composite reliability (CR) and average variance extracted (AVE). Statistical findings in this regard indicated that all principles have Cronabch's alpha (α) value above the cut-off point of 0.70 reneging between 0.94 for privacy and 0.96 for security by the same token, CR for all principles existed within their respective level of 0.70 as reported by Hair *et al.* (2010). Table IV indicates that while the highest of CR (0.906) was noticed for the security, the minimum value was exhibited by availability of AIS

Demographic characteristics	No.	(%)
Type of sector		
Service	162	0.68
Industries	77	0.32
Size: Number of employees		
>100 employees	92	0.38
≤100 employees	147	0.62
Experience: Number of years in business		
>10 years	96	0.40
≤10 years	143	0.60
Total	239	100

Table I. Demographic characteristics of the study's respondents

Table II.
Measurement items for SysTrust

The main principles	Selected items measures	References
Availability	Polices for minimizing risk system downtime; Data backup, and restoration Incremental backup and differential backup Disaster plan recovery Business continuity planning	AICPA, (2013; 2017); Greenberg, *et al.* (2012) Saito, (2001) Bedard, *et al.* (2005).
Security	IT security policy and producers Security awareness, and communication Logical access; Physical access Security monitoring User authentication; Incident management Systems development, and maintenance Personnel security; Configuration management; Change management Monitoring, and compliance	AICPA (2013; pp. 2-17); Abu-Musa, (2010); Saito, (2001).
Confidentiality	Confidentiality policy; confidentiality of inputs; confidentiality of data processing confidentiality of outputs Information disclosures (including third parties) Confidentiality of information in systems development	AICPA, (2013), Saito, (2001); Boritz, (2005).
Integrity processing	System processing integrity policies Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs. Information tracing from source to disposition	AICPA, (2013, 2017); Greenberg, *et al.* (2012), Saito, (2001); Bedard, *et al.* (2005).
Privacy	It defines documents, communicates, and assigns accountability for its privacy policies and procedures It provides notice about its privacy policies and procedures It describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information It collects personal information only for the purposes identified in the notice. It limits the use of personal information to the purposes identified in the notice It provides individuals with access to their personal information for review and update It discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual It maintains accurate, complete, and relevant personal information for the purposes identified in the notice	AICPA, (2013, 2017); Greenberg *et al.* (2012), Boritz, (2005).

Table III.
CR and AVE

Latent construct	Cronbach's alpha (α)	CR	AVE
Confidentiality	0.948	0.879	0.646
Availability	0.943	0.832	0.555
Privacy	0.945	0.897	0.686
Integrity Processing	0.949	0.873	0.633
Security	0.965	0.901	0.694

(0.832). Moreover, as seen in Table III the AVE value of the latent constructs ranged from 0.555 (Availability of AIS to 0.694 (security) which all are above the cut-off value of 0.50 as recommended by Sekaran and Bougie, (2017).

Convergent validity

According to Hair *et al.* (2017), convergent validity is established when the Average Variance for all focal constructs was more than 0.50, which meets the first condition of achieving convergent. Explained (AVE) between the constructs is equal to, or exceeds, 0.5. The average variance explained validity. To achieve the second requirement of convergent validity, it was vital to consider the reliabilities of the measurements as means of providing evidence and support for the convergent validity of the constructs (Hair *et al.*, 2017). As presented in Table III, all the scales demonstrated an acceptable "high" reliabilities, with the Cronbach's coefficient alpha's exceeding the 0.70 threshold, as recommended by Nunnally and Bernstein (1994); thereby, satisfying the second requirement of convergent validity.

The extent of the implementation of SysTrust service principles

The measure of extent of SysTrust implementation requirements are the main five principles and criteria (i.e. the availability, security, integrity processing, confidentiality and privacy) implemented for assuring the reliability of AIS as an internal control method. The mean values, standard deviation and *t*-test are used here to determine whether these main principles of SysTrust being implemented by the business organizations in Jordan. Findings shown in Table IV indicate that the extent of SysTrust principles (together) being practiced is considered to be moderate (i.e. 74 per cent or 5.20), as their mean are more than the mean of the scale, which is 4 (mean of the scale = Σ Degrees of the *scale* 7 = 1 + 2 + 3 + 4 + 5 + 6 + 7/ 7 = 5.20).

Testing hypotheses

One-sample *t*-test is used to examine the first hypothesis in the study. The result in the above Table IV shows that (SysTrust) principles and criteria are significantly implemented as an internal control method for assuring the overall reliability of AIS among business organizations either taken separately or together. The ANOVA analysis technique is also used to examine the other hypotheses. To assess the differences among business organizations in terms of the implementation of SysTrust principles and criteria requirements based on their organization's demographic characteristics such as size, type of business, and business experience (age), one way analysis of variance (ANOVA) was used to compare the means of participants' extent of implementation of SysTrust principles and criteria requirements and determine if there are any significant differences among the types of business sectors, i.e. service vs. industrial.

SysTrust principles	Mean	Percentage	Standard deviation	Sig. (two-tailed)
Availability	5.1398	0.7342	0.86783	0.000
Security	5.5559	0.7937	0.91053	0.000
Integrity processing	5.2214	0.7459	0.76369	0.000
confidentiality	5.2184	0.7454	0.87010	0.000
Privacy	5.2254	0.7464	0.91306	0.000
Average implementation	5.2214	0.7459	0.75279	0.000

Table IV. The level of implementation of SysTrust principles in business organizations

As it is shown in Table V, there are significant differences among business originations in terms of the practice of SysTrust principles either taken separately or together due to their types of business sector (e.g. service vs industrial business) to which they belong. When compared, the extent of SysTrust being practiced among business organizations in terms of type of business (service companies vs. industrial companies), service companies were found at a significant edge over industrial companies on all the five constructs of SysTrust.

ANOVA test is also used to measure the differences among the business originations in terms of the extent of implementation of SysTrust principles and criteria requirements based on their size (number of employees). The results shown in Table VI indicate there are no significant differences among business organizations in terms of extent of implementation of SysTrust principles and criteria requirements due to their size. This result suggests that the business organization were not varied in the extent of implementation of SysTrust principles and criteria requirements either taken together or separately due to their size of business.

Furthermore, ANOVA is used to examine the difference among the business organizations in terms of in the extent of implementation of SysTrust principles and criteria requirements based on their business experience (age). The result revealed in Table VII that there are significant differences among business organizations in terms of in the extent of extent of implementation of SysTrust principles and criteria requirements either taken together or separately due to their business experiences.

SysTrust principles	Sum of squares	Df	Mean square	F	Sig.
Availability					
Between groups	12.125	2	6.063	8.395	0.000
Within groups	247.706	343	0.722		
Total	259.832	345			
Security					
Between groups	9.398	2	4.699	5.827	0.003
Within groups	276.627	343	0.806		
Total	286.025	345			
Integrity processing					
Between groups	4.249	2	2.124	3.700	0.026
Within groups	196.964	343	0.574		
Total	201.213	345			
Confidentiality					
Between groups	8.919	2	4.459	6.063	0.003
Within groups	252.272	343	0.735		
Total	261.190	345			
Privacy					
Between groups	12.383	2	6.192	7.716	0.001
Within groups	275.233	343	0.802		
Total	287.616	345			
Total (all together)					
Between groups	8.735	2	4.367	8.021	0.000
Within groups	186.775	343	0.545		
Total	195.510	345			

Table V.
The significance level of SysTrust implementation among groups of organizations based on their type of business

SysTrust principles	Sum of squares	Df	Mean square	F	Sig.
Availability					
Between groups	3.804	3	1.268	1.694	0.168
Within groups	256.027	342	0.749		
Total	259.832	345			
Security					
Between groups	4.232	3	1.411	1.712	0.164
Within groups	281.792	342	0.824		
Total	286.025	345			
Integrity processing					
Between groups	5.516	3	1.839	1.913	0.173
Within groups	195.697	342	0.572		
Total	201.213	345			
Confidentiality					
Between groups	3.629	3	1.210	1.606	0.188
Within groups	257.561	342	0.753		
Total	261.190	345			
Privacy					
Between groups	6.073	3	2.024	2.459	0.063
Within groups	281.543	342	0.823		
Total	287.616	345			
Total (all together)					
Between groups	4.232	3	1.411	2.522	0.058
Within groups	191.279	342	0.559		
Total	195.510	345			

Table VI. The significance level of SysTrust implementation among groups of organizations based on the size of business

Discussion and implications

One of the main objectives of this study is to explore to which extent the business organizations in Jordan implemented the SysTrust principles and criteria requirements as an internal control system for assuring the reliability of AIS. The results indicate that the extent of SysTrust principles being practiced is considered to be moderate (i.e. 74 per cent or 5.20). This implies that there are some variations among shareholdings companies in terms of their level of implementations of the principles of SysTrust as presented in Table (4). This might indicate that internal control's methods over the computerized accounting information systems in the Jordanian business organizations provide requirements of all principals to the AIS system. Mean values have shown that the Security principle is the highly implemented one (79 per cent). Assurance of system security implies that access is restricted to the physical components of the system, the logic functions the system performs, and the information stored in the system. This results are in consistent with prior studies such as Hayale and Abu Khadra, (2006), Abu-Musa, (2010), and Boritz (2005). It could be concluded that the IT infrastructure of the Jordanian business originations (i.e. shareholding companies included in this study) by its status qua is mature enough to provide the operational requirements for (SysTrust) principles and criteria. Such result supported by the results reached by Casolaro and Gobbi, (2004) Mansour *et al.* (2009, 2017), and Al Hanini (2015).

The second objective of the study is to compare differences among business organizations in terms of the SysTrust principles and criteria requirements as an internal

Table VII.
The significance level of SysTrust implementation among groups of organizations based on their experience in business*

SysTrust principles	Sum of squares	Df	Mean square	F	Sig.
Availability					
Between groups	4.413	3	2.471	1748	0.119
Within groups	242.419	342	0.638		
Total	259.832	345			
Security					
Between groups	1.853	3	0.618	0.743	0.527
Within groups	284.172	342	0.831		
Total	286.025	345			
Integrity processing					
Between groups	2.407	3	0.802	1.380	0.249
Within groups	198.806	342	0.581		
Total	201.213	345			
Confidentiality					
Between groups	4.195	3	1.398	1.861	0.136
Within groups	256.995	342	0.751		
Total	261.190	345			
Privacy					
Between groups	2.472	3	0.824	0.988	0.398
Within groups	285.144	342	0.834		
Total	287.616	345			
Total (all together)					
Between groups	3.379	3	1.126	2.005	0.113
Within groups	192.131	342	0.562		
Total	195.510	345			

control system for assuring the reliability of AIS being implemented based on their type of business, size and experience. Interestingly, the study found no significant differences among business organizations in the extent of the SysTrust principles and criteria requirements being implemented due to their size or experience. One explanation for this is that all of business originations in this study are shareholding companies and irrespective of their size or experience they have to approve the reliability of their accounting transactions for legality and auditing purposes. However, statistical significant difference was found based on the type of business sector. It was found that the extents of the SysTrust principles and criteria requirements being implemented were varied among business organizations due to their type of business. One explanation of the above findings is that regardless the size of business organizations or experience, it is possible to classify Jordanian business in terms of the extent of SysTrust principles being implemented based on their type of business (services vs. industrial).

Based on the above discussed findings, two outstanding conclusions can be made. First, the results indicate that the extent of SysTrust principles being implemented is considered to be moderate. The results also showed that the Security principle is the highly implemented one. This could be because securities of AIS issues have been given a propriety over other principles among shareholding companies to be implemented. Second, when compared, the extent of SysTrust principles being implemented among business organizations in terms of type of business (service companies vs. industrial companies) was found at a significant edge over industrial companies on five principles of SysTrust. This result might indicate that the service companies apply or give more attention to the requirements of SysTrust principle than the industrial companies. This might be due to the fact that service companies tend to be more technology-oriented and driven than industrial companies in Jordan (Mahadeen *et al.*, 2016). In their study of EDI, Khazanchi and Sutton (2001) give evidence of the requirement for systems assurance, illustrating that numerous companies enforcing these systems do not use them to full benefit. However, there are no significant differences in the implementation of principles of SysTrust among business organizations due to their size or experience.

The present study has important implications for studies aimed to SysTrust principles implementation in developing countries. However, explanations of several findings above indicate the importance of contextual factors (i.e. demographic characteristics) within organizations. This study provides some insights into the implementation of SysTrust principle as an internal control for assuring the reliability of AIS by Jordanian shareholding companies, which should help practitioners to acquire a better understanding of the current SysTrust principles status and implementation. However, several limitations should be considered when evaluating and generalizing the study's conclusions. The study was conducted in one country, Jordan. Although Jordan is a valid indicator of prevalent factors in the wider MENA region and developing countries, the lack of external validity of this research means that any generalizations of the research findings should be taken with caution. Future research can be orientated in other national and cultural settings and compared with the results of this study.

References

Abu Musa, A. (2004), "Investigating the security controls of CAIS in an emerging economy: an empirical study on the Egyptian banking industry", *Managerial Auditing Journal*, Vol. 19 No. 2, pp. 7-18.

Abu-Musa, A. (2010), "Information security governance in Saudi organizations: an empirical study", *Information Management and Computer Security*, Vol. 18 No. 4, pp. 226-276.

AICPA (2013), *National Conference on Current SEC and PCAOB Developments*.

AICPA (2017), *Trust Services Criteria*, AICPA Publishing.

AICPA/CICA (2006), "Trust services principles, criteria and illustrations for security, availability, processing integrity, confidentiality, and privacy (including WebTrust and SysTrust)", American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants, available at: www.webtrust.org/principles-and-criteria/item27818.pdf

Al Hanini, E. (2015), "Evaluating the reliability of the internal control on the computerized accounting information systems: an empirical study on banks operating in Jordan", *Research Journal of Finance and Accounting*, Vol. 6 No. 8, pp. 176-188.

Al-Laith, A. (2012), "Adaptation of the internal control systems with the use of information technology and its effects on the financial statements reliability: an applied study on commercial banks", *International Management Review*, Vol. 8 No. 1, pp. 12-82.

Amin, H. and Mohamed, E. (2016), "Auditors' perceptions of the impact of continuous auditing on the quality of internet reported financial information in Egypt", *Managerial Auditing Journal*, Vol. 31 No. 1, pp. 111-132.

Arens, A., Elder, R.J. and Beasley, M. (2014), *Auditing and Assurance Services: an Integrated Approach*, 15th ed., Boston- Prentice Hall.

Arnold, J., Lampe, J., Masselli, S. and Sutton, S. (2000), "An analysis of the market for systems reliability assurance services", *Journal of Information Systems*, Vol. 14 No. 1, pp. 65-82.

Bedard, J.C., Jackson, C.M. and Graham, L. (2005), "Issues and risks in performing SysTrust engagements: implications for research and practice", *International Journal of Accounting Information Systems*, Vol. 6 No. 1, pp. 55-79.

Boritz, J.E. (2005), "IS practitioners' view on core concepts of information integrity", *International Journal of Accounting Information Systems*, Vol. 6 No. 4, pp. 260-279.

Boritz, E. and Hunton, J. (2002), "Investigating the impact of auditor-provided systems reliability assurance on potential service recipients", *Journal of Information Systems*, Vol. 16 No. 1, pp. 69-88.

Boritz, J.E. and Kearns, J.H. (2000), "Symposium in IS assurance panel discussion on SysTrust", *Journal of Information Systems*, Vol. 14 No. 1, pp. 163-176.

Boritz, E., Mackler, E. and McPhie, D. (1999), "Reporting on systems reliability", *Journal of Accountancy*, Vol. 188 No. 5, pp. 75-83.

Burton, F., Emett, S., Simon, C. and Wood, D. (2012), "Corporate managers' reliance on internal auditor recommendations", *Auditing: A Journal of Practice and Theory*, Vol. 31 No. 2, pp. 151-166.

Casolaro, L. and Gobbi, G. (2004), "Information technology and productivity changes in the Italian banking industry", *Report Published by Bank of Italy Economic Research Department*, pp. 1-26.

Cerullo, M. and Michael, J. (1999), "Client/server systems security and controls", *Internal Auditor Journal*, Vol. 56.

Chang, Y.W. (2001), "Contingency factors and accounting information system design in Jordanian companies", *Journal of Accounting Information System*, Vol. 8, pp. 1-16.

Committee of Sponsoring Organizations of the Treaway Commission (COSO) (2013), "COSO internal control – integrated framework", KPMG International.

Daneila, M, Vassen, E, H.J., Dameri, R.P. (Eds), (2013), *Accounting Information System for Decision Making*, Springer-Verlag, Berlin.

Davila, A. and Foster, G. (2005), "Management accounting systems adoption decisions: evidence and performance implications from early-stage/startup companies", *The Accounting Review*, Vol. 80 No. 4, pp. 1039-1068.

Doms, M.E., Jarmin, R.S. and Klimek, S.D. (2004), "Information technology investment and firm performance in US retail trade", *Economics of Innovation and New Technology*, Vol. 13 No. 7, pp. 595-613.

Douglas, N.K. (2011), "Internal control and its contributions to organizational efficiency and effectiveness: a case study of Ecobank Ghana Limited", available at: http://ir.knust.edu.gh/handle/123456789/4210

El-Sayed, A. and Hassan, I. (2010), "Advanced auditing in the contemporary business environment", Faculty of Commerce – Alexandria University (in Arabic).

Elliott, R.K. (1995), "The future of assurance services: implications of academia", *Accounting Horizons*, Vol. 9 No. 4, pp. 118-127.

Enofe, A., Amaria, P. and Anekwu, D. (2012), "Major changes affecting the accounting profession: empirical investigation", *International Journal of Business and Public Administration*, Vol. 9 No. 2, pp. 77-96.

Fortesa, N. and Ritab, P. (2016), "Privacy concerns and online purchasing behaviour: towards an integrated model", *European Research on Management and Business Economics*, Vol. 22 No. 3, pp. 167-176.

Gray, G.L. (2002), "Discussion of investigating the impact of auditor-provided systems reliability assurance on potential service recipients", *Journal of Information Systems*, Vol. 16, pp. 91-96.

Greenberg, R., Li, W. and Wing, B. (2012), "The effect of trust in system reliability on the intention to adopt online accounting systems", *International Journal of Accounting and Information Management*, Vol. 20,No. 4, pp. 363-376.

Hair, Jr, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010), *Multivariate Data Analysis: A Global Perspective*, 7th ed, Pearson Education International.

Hair, J.F., Hult, J.M., Ringle, C. and Sarstedt, M. (2017), *A Primer on Partial Least Squares Structural Equation Modelling (PLS-SEM)*, 2nd ed., SAGE Publications, Thousand Oaks, CA.

Havelka, D., Sutton, S.G. and Arnold, V. (1998), "A methodology for developing measurement criteria for assurance services: an application in information systems assurance", *Auditing: A Journal of Practice and Theory*, pp. 73-92.

Hayale, H. and Abu Khadra, A. (2006), "Evaluation of the effectiveness of control systems in computerized accounting information systems: an empirical research applied on Jordanian banking sector", *Journal of Accounting Business Management*, Vol. 13 No. 3, pp. 39-68.

Henry, L. (1997), "A study of the nature and security of accounting information systems: the case of Hampton Roads, Virginia", the Mid-Atlantic", *Journal of Business*, Vol. 33 No. 63, pp. 171-189, available at: www.aicpa.org/assurance/scas/comstud/defincom/index.htm

Hunton, J.E., Benford, T., Arnold, V. and Sutton, S.G. (2000), " "The impact of electronic commerce assurance on financial analysts' earnings forecasts and stock price estimates", *Auditing: A Journal of Practice and Theory*, Vol. 18, pp. 5-22.

Iceman, R. and Hillson, J. (2012), "Distribution of audited detected errors partitioned by internal control", *Journal of Accounting, Auditing and Finance*, Vol. 5 No. 4, pp. 527-543.

Jamal, K. and Maier, M. (2002), "Can WebTrust survive?", Working paper, University of Alberta.

Joseph, C., Steve, G., Sutton, J. and Kuhn, R., Jr, (2009), "The pervasive nature of IT controls: an examination of material weaknesses in IT controls and audit fees", *International Journal of Accounting and Information Management*, Vol. 17 No. 1, pp. 106-119.

Kaplan, S.E. and Nieschwietz, R.J. (2003), "A web assurance services model of trust for B2C e-commerce", *International Journal of Accounting Information Systems*, Vol. 4 No. 2, pp. 95-114.

Khazanchi, D. and Sutton, S. (2001), "Assurance services for business-to-business electronic commerce: a framework and implications", *Journal of the Association for Information Systems*, Vol. 1 No. 11, pp. 1-53.

Kim, H., Hoskisson, R.E. and Wan, W.P. (2004), "Power dependence, diversification strategy, and performance in keiretsu member firms", *Strategic Management Journal*, Vol. 25 No. 7, pp. 23-34.

Knechel, W., Wallage, P., Eilifsen, A. and Praag, B. (2006), "The demand attributes of assurance services providers and the role of independent accountants", *International Journal of Auditing*, Vol. 10 No. 2, pp. 143-162.

Kovar, S.E. and Mauldin, E.G. (2003), "Antecedents of demand for assurance services: a model for analysis with applications in B2B E-Commerce", Working paper, The University of Missouri – Columbia.

Kuhn, J.R., Jr, Ahuja, M. and Mueller, J. (2013), "An examination of the relationship of IT control weakness to company financial performance and health", *International Journal of Accounting and Information Management*, Vol. 21 No. 3, pp. 227-240.

McCole, P., Ramsey, E. and Williams, J. (2010), "Trust considerations on attitudes towards online purchasing: the moderating effect of privacy and security concerns", *Journal of Business Research*, Vol. 63 Nos 9/10, pp. 10 pp., 1018-1024.

McPhie, D. (2000), "*Information Systems Assurance and Advisory Services*", Ernst and Young.

Mahadeen, B., Al-Dmour, R., Obeidat1, B. and Tarhini, A. (2016), "Examining the effect of the organization's internal control system on organizational effectiveness: a Jordanian empirical study", *International Journal of Business Administration*, Vol. 7 No. 6, pp. 22-34.

Mansour, E.A., Salamat, W. and Masadeh, W. (2017), "The impact of reliability elements on performance indicators of Jordanian", *The International Journal of Business and Finance Research*, Vol. 11 No. 1, pp. 87-107.

Mansour, E.A., Salamat, W. and Masadeh, W. (2009), "Examine the existence of (SysTust) model and its impact on commercial banks performance", *European and Mediterranean Conference on Information Systems*, Vol. 2, pp. 31-38.

Martin, J. (2005), "Trust services: a better way to evaluate IT controls", *Journal of Accountancy*, Vol. 199 No. 3, pp. 34-40.

Mauldin, E.G., Nicolaou, A. and Kovar, S.E. (2006), "The influence of scope and timing of reliability assurance in B2B E-Commerce", *International Journal of Accounting Information Systems*, Vol. 7 No. 2, pp. 115-129.

Meharia, P. (2012), "Assurance on the reliability of mobile payment system and its effects on its 'use': an empirical examination", *Accounting and Management Information Systems*, Vol. 11, pp. 97-111.

Nelson, R.R., Todd, P.A. and Wixom, B.H. (2005), "Antecedents of information and system quality: an empirical examination within the context of data warehousing", *Journal of Management Information Systems*, Vol. 21 No. 4, pp. 199-209.

Nunnally, J.C. and Bernstein, H. (1994), *Psychometric Theory*, 3nd ed., McGraw-Hill, New York, NY.

Perego, P. (2009), "Causes and consequences of choosing different assurance providers: an international study of sustainability reporting", *International Journal of Management, December*, Vol. 26 No. 3, pp. 412-425.

Pugliese, A. and Hales, R. (2000), "SysTrust and WebTrust: technology assurance opportunities", *The CPA Journal*, Vol. 70 No. 11, pp. 28-34.

Qurashi, A. and Siegel, J. (1997), "The accountant and computer security", *National Public Accountant Journal*, Vol. 42 No. 3, pp. 26-44.

Raupeliene, A. and Stabingis, L. (2003), "Development of a model for evaluating effectiveness of accounting information systems", *Efate Conference, EFITA Conference*, pp. 339-345.

Romney, M.B. and Steinbart, P.J. (2017), '*Accounting Information Systems*, 14th ed., Pearson Prentice Hall. New York, NY.

SACF (2001), *Information Security Governance Guidelines for Boards of Directors and Executive Management*, 2nd ed., IT Governance Institute, USA.

Saito, T. (2001), "Translation SysTrust; principles and criteria for systems reliability version 1.0", *Journal of Tokyo University of Information Sciences*, Vol. 4 Nos 2/3, pp. 140-147.

Sekaran, U. and Bougie, R. (2017), *Research Methods for Business: A Skill Building Approach*, 7th Edition, Wiley.

Siponen, M.T. and Oinas-Kukkonen, H. (2007), "A review of information security issues and respective research contributions", *ACM SIGMIS Database*, Vol. 38 No. 1, pp. 60-80.

Strong, D.M., Lee, Y.W. and Wang, R.Y. (1997), "Data quality in context", *Communications of the Acm*, Vol. 40 No. 5, pp. 103-110.

Tan, Y. and Theon, W. (2002), "Toward a generic model of trust for electronic commerce", *International Journal of Electronic Commerce*, Vol. 5 No. 2, pp. 61-74.

Tarek, M., Mohamed, E.K.A., Hussain, M.M. and Basuony, M.A.K. (2017), "The implication of information technology on the audit profession in developing country: extent of use and perceived importance", *International Journal of Accounting and Information Management*, Vol. 25 No. 2, pp. 237-255.

Topash, N.K. (2014), "Evaluation of efficiency of accounting information systems: a study on mobile telecommunication companies in Bangladesh", *Global Disclosure of Economics and Business*, Vol. 3 No. 1, pp. 40-55.

Warren, M.J. (2002), "Security practice: survey evidence form three countries", *Logistics Information Management*, Vol. 15 Nos 5/6, pp. 347-351.

Yigitbasioglu, O. (2016), "Firms' information system characteristics and management accounting adaptability", *International Journal of Accounting and Information Management*, Vol. 24 No. 1, pp. 20-37.

Zhou, T. (2011), "Examining mobile banking user adoption from the perspectives of trust and flow experience", *Information Technology and Management*, Vol. 13 No. 1, pp. 27-37.

Further Reading

AICPA/CICA Systems Reliability Task Force (2000), "AICPA/CICA SYSTRUST^{TM} Principles and Criteria", *Journal of Information Systems*, Vol. 14, No. 1, pp. 1-7.

Bagozzi, R.P. and Yi, Y. (1988), "On the evaluation of structural equation models", *Journal of the Academy of Marketing Science*, Vol. 16 No. 1, pp. 74-94.

Elliott, R.K. and Pallais, D.M. (1997), "Are you ready for new assurance services?", *Journal of Accountancy*, Vol. 183 No. 6, pp. 47-51.

Havelka, W., Henderson, A. and Oesterhelt, R. (1995), "Three-dimensional structure of halo -rhodopsin at 7 Å resolutions", *Journal of Molecular Biology*, Vol. 247 No. 4, pp. 726-738.

Kovar, S.E., Burke, K.G. and Kovar, B.R. (2000), "Consumer responses to the CPA WEBTRUST assurance", *Journal of Information Systems*, Vol. 14 No. 1, p. 17.

Mauldin, E. and Arunachalam, V. (2002), "An experimental examination of alternative forms of web assurance for business-to-consumer e-Commerce", *Journal of Information Systems*, Vol. 6 No. 1, pp. 33-54.

Netemeyer, R.G., Bearden, W.O. and Sharma, S. (2003), *Scaling Procedures: issues and Applications*, Sage Publications, Thousand Oaks.

Odom, M.D., Kumar, A. and Saunders, L. (2002), "Web assurance seals: how and why they influence consumers' decisions", *Journal of Information Systems*, Vol. 16 No. 2, pp. 231-250.

Papazoglou, M. and Tsalgatidou, A. (2000), "Editorial: business to business electronic commerce issues and solutions", *Decision Support Systems*, Vol. 29 No. 4, pp. 301-304.

Teo, T. and Liu, J. (2007), "Consumer trust in e-commerce in the United States, Singapore and China", *Omega: International Journal of Management Science*, Vol. 35 No. 1, pp. 22-38.

Corresponding author

Hani H. Al-Dmour can be contacted at: dr_dmourh@yahoo.com