Addressing Information Security Risks by Adopting Standards

Walid Al-Ahmad*‡, Bassil Mohammad**

*Computer Science Department, Faculty of Arts and Science, Gulf University for Science & Technology, Kuwait

**Ernst & Young, Amman, Jordan

‡P.O.Box 7207 Hawally, 32093 Kuwait, Tel: +96525307321, Fax: +965 25307030, e-mail: alahmed.w@gust.edu.kw

Abstract- Modern society depends on information technology in nearly every facet of human activity including, finance, transportation, education, government, and defense. Organizations are exposed to various and increasing kinds of risks, including information technology risks. Several standards, best practices, and frameworks have been created to help organizations manage these risks. The purpose of this research work is to highlight the challenges facing enterprises in their efforts to properly manage information security risks when adopting international standards and frameworks. To assist in selecting the best framework to use in risk management, the article presents an overview of the most popular and widely used standards and identifies selection criteria. It suggests an approach to proper implementation as well. A set of recommendations is put forward with further research opportunities on the subject.

Keywords- Information security; risk management; security frameworks; security standards; security management.

1. Introduction

The use of technology is increasingly covering most aspects of our daily life. Businesses which are heavily dependent on this technology use information systems which were designed and implemented with concentration on functionality, costs reduction and ease of use. Information security was not incorporated early enough into systems and only recently has it started to get the warranted attention. Accordingly, there is a need to identify and manage these hidden weaknesses, referred to as systems vulnerabilities, and to limit their damaging impact on the information systems integrity, confidentiality, and availability. Vulnerabilities are exploited by attacks which are becoming more targeted and sophisticated. Attacking techniques and methods are virtually countless and are evolving tremendously [1, 2].

In any enterprise, information security risks must be identified, evaluated, analyzed, treated and properly reported. Businesses that fail in identifying the risks associated with the technology they use, the people they employ, or the environment where they operate usually subject their business to unforeseen consequences that might result in severe damage to the business [3]. Therefore, it is critical to establish reliable information security risk assessment and treatment frameworks to guide organizations during the risk management process.

Because risks cannot be completely eliminated, they need to be reduced to acceptable levels. Acceptable risks are risks that the business decides to live with, given that proper assessment for these risks has been performed and the cost of treating these risks outweighs the benefits.

To this effect, enterprises spend considerable resources in building proper information security

risk management programs that would eventually address the risks they are exposed to. These programs need to be established on solid foundations, which is the reason why enterprises look for standards and frameworks that are widely accepted and common across enterprises [4]. However, the fact that several standards and frameworks exist make it challenging for enterprises to select which one to adopt and the question: "which is the best?" warrants further investigation. The main objective of this paper is to provide an answer to this question, thereby assisting enterprises in developing proper understanding of the issue and establishing successful information security risk management programs. This paper provides an analysis of some existing standards and frameworks for information security risks and consolidates various aspects of the topic. It also presents the challenges that frustrate information security risk management efforts along with how leading market standards and practices can be used to address information security risks with insights on their strengths and weaknesses.

Please note that the scope of this paper is limited to the following frameworks: ISO 27001, ISO 27002, ISO 27005, ITIL, COBIT, Risk IT, Basel II, PCI DSS, and OCTAVE. These are the most commonly used frameworks in the market [5]. Other frameworks and methodologies like RMF (by NIST) and M_o_R (by GOC) can be considered in future work. It is also important to mention that this paper is not intended to promote a specific standard or framework; rather it treats them equally. Conclusions drawn as a result of this work are based on our detailed analyses, research, literature review, and observations from our work experience and engagements with clients from various sectors in the field of information security.

The remainder of this paper is organized as follows: section 2 highlights some related work; section 3 details some challenges that disturb information security risk assessments; section 4 provides an overview of the major drivers for standards adoption; section 5 provides detailed analyses and exploration for the standards and frameworks in scope; section 6 details with the strengths and weaknesses of these standards and frameworks when used as a means to address information security risks; section 7 captures the selection considerations to use; section 8 provides some recommendations along with the proposed approach; section 9 presents a case study to illustrate the benefits of the proposed selection method; finally, section 10 puts forward some conclusions and future research opportunities in relation to our work.

2. Related Work

The literature on information security risk management based on international standards is scarce. The literature lacks studies that guide organizations in selecting the standard that fits their needs. Some research works attempt to analyze existing information security risk management standards, mainly ISO 27001 [6]. However, these research works focus mainly on listing advantages and disadvantages of these standards and how to implement and manage them. No comprehensive studies have been done to holistically compare various frameworks, with the objective of providing selection criteria for the best standard or proposing a better assessment approach. Some papers dealt with frameworks such as COBIT, ITIL, and ISO 17799, as means to manage compliance requirements [7]. Ref. [8] proposes a framework which considers global, national, organizational, and employee standards to guide information security management. Ref. [9] presents framework of information security standards conceptualization, interconnection and categorization to raise awareness among organizations about the available standards (mainly ISO series).

As well as exploring existing frameworks used in IT risk management this paper presents the challenges facing organizations to successfully implement information security risk assessments and the drivers for standards adoption. The main and novel contribution of our research work is the proposal of a practical approach to selecting an appropriate framework to address information security risks.

3. Challenges to Information Security Risk Assessments

Some of the common challenges to information security risk assessments are discussed briefly in this section. In fact, these challenges represent critical failure factors for an information risk management program.

1) Absence of senior management commitment & support: Management's buy-in and support is a critical driver for the success of any IT project, including information security risk assessments. Absence of management commitment will result in wasting valuable resources and efforts, producing weak evaluations, and most importantly, will lead to ignoring the assessment findings [10].

2) Absence of appropriate policies for information security risk management: It is crucial to have information security policies in place to reflect the enterprise objectives and management directions. Although some policies might be created, information security risk management policies tend to be dropped or forgotten. In a research conducted by GAO, the US Government Accountability Office, three out of four detailed case studies showed that despite the fact that firms used to have some form of information security risk assessment approaches practiced for several years, the risk management and assessment policies and processes were not documented until recently [11]. The absence of this critical steering document will lead to unstructured risk assessment approaches and will openly allow unmanaged evaluations.

3) Disintegrated GRC efforts: The increasingly popular term GRC refers to three critical areas: Governance, Risk Management, and Compliance. According to COBIT 4.1, IT Governance is defined as "the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives" [12]. Risk management is a process through which management identifies, analyses, evaluates, treats, communicates, and monitors risks that might adversely affect realization of the organization's business objectives. Compliance is about making sure that external laws, regulations, mandates and internal policies are being complied with at a level consistent with corporate morality and risk tolerance. Governance, risk, and compliance should always be viewed as a continuum of interrelated functions, best approached in a comprehensive, integrated manner. The disintegration results in increased failure rates, waste of resources, and increased overall assurance cost.

4) Improper assessments management: Despite the importance of security risk assessments, they are mostly not managed as projects and merely considered as part of IT normal operations. Considering security risk assessments as part of IT routine assignments will exclude these assessments from business review and consequently will result in a definite disconnect between management and their enterprise information security assessments. This exclusion will also increase the possibilities of executing over-budget assessments that will only cause additional efforts and resources to be wasted.

5) Assets ownership is either undefined or unpracticed: In ISO 27001 "the term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. [13]. This definition entails major responsibility granted to the person who is assigned the ownership which includes making sure that proper controls are actually implemented in order to protect the asset. Information security standards, best practices and mandates like ISO, COBIT, and ITIL require that information assets are identified, inventoried, and ownership is assigned. This is crucial for the success of any information security assessment. Most organizations fail to develop comprehensive information assets inventories and accordingly do not assign ownership [14].

6) Limitations of existing automated solutions: Software solutions for information security risk assessment are developed to aid in the automation of this process and to make it more efficient. In a detailed comparison conducted by "Risk Assessment Accelerator", seven common solutions were compared with respect to more

than forty different areas [15]. Features like ease of use, multi-language and client-server architecture support were highlighted as existing limitations in four up to five of these solutions. Three out of the seven compared solutions provide limited customization capabilities for both built-in inventories (for risks, vulnerabilities and threats) and the generated dashboards. All these weaknesses and limitations degrade enterprises' efforts to have efficient and reliable information security risk assessment requirements documentation.

7) Existence of several IT risk assessment frameworks: The existence of many information security risk management and assessment frameworks add to the ambiguity and challenge of what is the best one to use. As a matter of fact, analyses of exiting risk assessment frameworks show that there is no one-size-fits-all solution to this issue as it is hard to develop a single precise document that will address the needs of all enterprises given their variant natures and requirements.

4. Drivers for Standards Adoption

In order to address their information security risk management and assessment challenges, enterprises adopt internationally accepted frameworks or best practices. Standards in general are meant to provide uniformity that would ease the understanding and management of concerned areas. Businesses find themselves in need to adopt standards for various reasons which vary from business requirements to regulators and compliance mandates. Establishment of proper corporate governance, increasing risk awareness and competing with other enterprises are some business drivers to mention. Some firms pursue certifications to meet market expectations and improve their marketing image. A major business driver for standards adoption is to fill in the gaps and lack of experience in certain areas where firms are not able to build or establish proprietary standards based on their staff competencies [16].

Providing confidence to trading partners, stakeholders, and customers, reducing liability due to unimplemented or enforced policies and procedures, getting senior management ownership and involvement and establishing a mechanism for measuring the success of the security controls are some other key drivers for the adoption of standards.

5. Leading Market Best Practices Standards

The conclusion section should emphasize the main contribution of the article to literature. Authors may also explain why the work is important, what are the novelties or possible applications and extensions. Do not replicate the abstract or sentences given in main text as the conclusion.

In this section, an overview is presented of a number of the more important standards for information security risk management. For detailed information about these standards, the reader is encouraged to consult the references provided for them. The list of standards presented is absolutely not complete, and as mentioned before a subset of the existing standards are treated in this paper.

5.1. ISO 27000 Set

The ISO 27000 is a series of standards, owned by the International Standards Organization, focusing on information security matters. For the purposes of this work, ISO 27001, ISO 27002, and ISO 27005 will be explored to highlight their strengths and weaknesses in relation to current demands for effective and robust frameworks for information security risk assessments.

ISO 27001: The ISO 27001 standard is the specification for an Information Security Management System (ISMS). The objective of the standard is to specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System within an organization [13]. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets. It is seen as an internationally recognized structured methodology dedicated to information security management.

The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA cycle has these four phases:

- Plan – establishing the ISMS
- Do – implementing and operating the ISMS
- Check – monitoring and reviewing the ISMS
- Act – maintaining and improving the ISMS

Organizations that adopt ISO 27001 in their attempt to pursue an effective means for operational information security risk management overlook the fact that this standard was designed to be used mainly as an ISMS framework – at the high level, not operational level - founding proper bases for information security management. ISO 27001 document mentions valuable details on information security risk assessment – mainly in the statements 4.2.1.C thru 4.2.1.H that can be used as selection criteria for a proper information security risk assessment approach that builds upon the controls list proposed by the standard.

ISO 27002: ISO 27002 is a code of practice that provides suggested controls that an organization can adopt to address information security risks. It can be considered an implementation roadmap or extension to ISO 27001. As stated in the standard document, the code of practice is established to provide "guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization" [17]. The controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities" [18]. ISO 27002 as the Code of Practice is best suited to be used as a guidance and direct extension to ISO 27001. ISO 27002 is used by enterprises as the sole source of controls and a means for information security risk assessment, however, not all controls are mandated as firms' structures and businesses vary. Controls selection must be done based on detailed and structured assessment to determine which specific controls are appropriate and which are not.

This standard contains guidelines and best practices recommendations for these 10 security domains: Security Policy; Organization of Information Security; Asset Management; Human Resources Security; Physical and Environmental Security; Communications and Operations Management; Access Control; Information Systems Acquisition, Development and Maintenance; Information Security Incident Management; Business Continuity Management; and Compliance.

Among these 10 security domains, a total of 39 control objectives and hundreds of best-practice information security control measures are recommended for organizations to satisfy the control objectives and protect information assets against threats to confidentiality, integrity and availability.

ISO 27005: ISO 27005 standard was proposed to fill in the gaps existing in ISO 27001 and ISO 27002 in terms of information security risk management. The standard builds up on the core that was introduced in ISO 27001 – reference statements 4.2.1.C thru 4.2.1.H – and elaborates by identifying inputs, actions, implementation guidelines, and outputs for each and every statement. However, during our research we realized that the adoption of this standard as a means for information security risk management is minimal. This was evident in "The Open Group" efforts to support ISO 27005 adoption by releasing a free detailed technical document – called ISO/IEC 27005 Cookbook – that uses ISO 27005 as a cornerstone for a complete risk management methodology [18, 19]. ISO 27005 is not intended to be an information security risk assessment methodology [20].

The standard has six annexes that are all informative but considered of a major value extension to the standard. With proper customization, these annexes along with the ISO 27005 body can be used as the main assessment methodology for security risks.

5.2. IT Infrastructure Library (ITIL 3.0)

ITIL is one of the IT frameworks used as a best practice adopted to properly manage IT services. ITIL perceives any effort or action done by IT in support to the organization as a service that has value to customers or businesses. The ITIL library focuses on managing IT services and covers all aspects of IT service provisioning starting from service strategy, design, transition, operation, and implementation. It also highlights the continual monitoring and improvement aspect for each and every service.

ITIL does not introduce itself as a framework for information security risk management. However, as an IT governance framework, having it implemented in an enterprise will provide assurance and indication on the organization's IT maturity. Addressing IT risks associated with incident, change, event, problem, and capacity management would definitely minimize related information security risks as well [21, 22].

The drivers for ITIL adoption in organizations were subject to analyses and study by several researches. A survey conducted by itSMF (IT Service Management Forum) showed that ITIL was adopted by different industry sectors [23] including education, government, and financial sectors amongst others. The ITIL status survey for 2009 [24] showed the increasing adoption of ITIL version 3.0 and elaborated on the major drivers that are causing this adoption. This includes improving service quality, customer satisfaction and establishing IT stability and successful value delivery for business. ITIL modularity adds to its adoption popularity. Based on the enterprise current priorities, the firm can select to focus on service operations rather than service strategy which typically needs more time to mature. The implementation of ITIL can be implemented gradually in phases.

5.3. COBIT 4.1 & Risk IT

Control Objectives for Information and related Technology (COBIT), developed and owned by the Information Systems Audit & Control Association (ISACA), is one of the most increasingly adopted information technology frameworks for IT Governance. COBIT focuses on defining IT control objectives and developing the controls to meet them. It is made of 34 processes that manage and control information and the technology that supports it [12].

COBIT is adopted by enterprises from various industry sectors [25] which include IT consulting firms, education, financial institutions, government, healthcare, utilities and energy. To get closer understanding on how various enterprises perceive COBIT, thirty case studies were reviewed and analyzed. The case studies showed that COBIT was used to create the needed alignment between business and IT, create the IT Governance framework, improve IT processes and establish the IT risk management organization. Other enterprises used COBIT to meet their compliance needs and requirements. It was realized from the case studies that financial institutions adopt COBIT for their internal IT audit efforts and risk assessments. They also used it to create IT policies and procedures. Other firms used COBIT as a means to standardize IT processes and increase their effectiveness and maturity level. COBIT was also used as a means to conduct audit. COBIT does not provide a methodology to conduct information security risk assessments but rather establishes the foundation for having a solid IT organization in the firm.

ISACA recognized the importance and need for a comprehensive IT risk management framework and as a result developed the Risk IT framework. According to the Risk IT framework document "The Risk IT framework complements ISACA's COBIT, which provides a comprehensive framework for the control and governance of business-driven IT-based solutions and services. While COBIT sets good practices for the means of risk management by providing a set of controls to mitigate IT risk, Risk IT sets good practices for the ends by providing a framework for enterprises to identify, govern and manage IT risks [26].

Risk IT provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues. It enables enterprises to understand and manage all significant IT risk types. Risk IT follows the process model used in COBIT and has three major domains: 1) Risk Governance which

focuses on the establishment and maintenance of common risk view, and making risk-aware business decisions; 2) Risk Evaluation which deals with data collection, risks analyses and maintaining risk profile; 3) The Risk Response component articulates risk, manages risk and reacts to all adverse events identified [26].

Given that Risk IT is still new, its adoption across enterprises is not yet realized, however, it is expected to take more attention and focus in the near future taking use of the wide acceptance and adoption of COBIT.

5.4. Other Frameworks

In this section, we briefly discuss other standards and regulations for information security. Some industries, such as banking, are regulated, and the guidelines or best practices put together as part of those regulations often become a de facto standard among members of these industries.

Basel II: Basel II is the most commonly adopted directive across the financial institutions. The reason behind this is the fact that this directive has become a mandated regulation that all financial institutions need to comply with. Its core is about how much capital banks need to put aside to guard against the types of financial and operational risks banks face [27]. It focuses on operational risks as opposed to information security risks. According to Basel II, operational risk (Ops Risk) is any risk that results from failure in any of the following areas: system, process, human or external attack. This definition implies that Basel II has an IT dimension that needs to be properly managed. This area was subject for detailed research and several publications tried to set clear controls and control objectives to mitigate the related risks. ISACA led this effort and developed a detailed framework in this regards [28].

PCI DSS: Payment Card Industry Data Security Standard (PCI DSS) [29], currently in version 2.0, is a standard that consists of twelve domains and was created by payment brands leaders to help facilitate the broad adoption of consistent data security measures on a global basis. Proper implementation of PCI DSS assists in building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, and implementation of solid access control measures. Compliance with PCI requirements is mandated for any party that stores or transmits credit or debit card data. It assists enterprises to manage information security risks, reduces losses resulting from fraud, and protects consumer data. PCI DSS is not intended to be used as an information security risk management or assessment framework; however, while efforts are spent towards fulfilling its requirements overall information security maturity level is leveraged making it easier to achieve better security assessments. For organizations that already have ISMS (ISO 27001) implemented, PCI DSS compliance is straight forward.

OCTAVE Set: OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), developed at the CERT Coordination center at Carnegie Mellon University, is a detailed information security risk assessment methodology; it consists of tools, techniques and methods to conduct risk assessments. It is a formal and detailed set of processes, which assist in ensuring that risks are identified and properly analyzed, following the standard techniques used in most risk analysis procedures. However, due to the level of activity and overhead involved in OCTAVE, it is probably best suited to large organizations or projects. It has three models that are carefully developed to fit into various enterprises needs [30]. There are three OCTAVE methods:

- the original OCTAVE method, which forms the basis for the OCTAVE body of knowledge
- OCTAVE-S, for smaller organizations
- OCTAVE-Allegro, a streamlined approach for information security assessment and assurance

The OCTAVE Method Implementation Guide provides everything that an analysis team needs to use the OCTAVE Method to conduct an evaluation in their organization. It includes a complete set of detailed processes, worksheets, and instructions for each step in the method, as well as support material and guidance for tailoring.

6. Strengths and Weaknesses

Several researches tried to identify shortcomings and limitations associated with standards which impact their adoption [31]. Despite that a lot of research was related to ISO 27000 standards, mainly ISMS and its code of practice ISO 27002; we found that most of the reported items were easily realized in other frameworks as well. Issues like high implementation costs, lack of skilled people, and standards generality are some of these common items that were found in all the previously discussed standards with the exception of OCTAVE.

For most SMEs (Small-Medium Enterprises) costs for standards implementation are hard to justify especially when senior management is insufficiently concerned about information security, and associated risks are continuously underestimated. Accordingly, large enterprises lead the statistics in standards adoption compared with SMEs [31]. The standards generality, on the other side, does not count for differences in enterprises security risk requirements and might result into inconsistent interpretations by various parties.

Complexity and lack of guidance is another limitation found in several standards. For example, using the ISO 27001 standard source document alone is not sufficient to implement an effective ISMS organization. This is where detailed guidelines are needed as various processes and controls are merely described in the standard without detailing the "how to" implement for practitioners. Providing detailed guidelines for standards and best practices surfaced as a need to assist in better understanding and to encourage more adoption. ISACA has done this for its frameworks. "Risk IT Practitioner Guide" and various COBIT publications support Risk IT and COBIT. The Office of Government Commerce (OGC) has done the same for ITIL through the release of their complete library of publications that details how to effectively implement ITIL. The PCI Council continuously releases explanations and guidelines for PCI DSS implementation. A step-by-step detailed manual on how to use OCTAVE was made available as well [30]. ISO 27003 was introduced recently to cover the need for guidance for ISO 27001 and ISO 27002.

From our observations through engagements with clients, we realized a considerable acceptance for COBIT framework as a means to achieve various objectives. For various industries, COBIT assists in structuring IT governance and risk management, ensuring business-IT objectives alignment, standardizing IT processes, unifying processes and ensuring IT management quality. Because of its process-based structure, availability of detailed controls and controls objectives, and potential to automate; COBIT is used as a structured audit approach for internal IT audits. Most importantly, it is best selected for mergers and acquisitions reviews and compliance with external (e.g. regulators, organizations or third-party) requirements. In addition to its risk management focused framework, Risk IT, COBIT is a complete and comprehensive framework to adopt in order to establish solid IT organization.

Like other frameworks, COBIT's complexity is limiting its adoption in some enterprises that lack the expertise and budgets for its implementation. In order to address this concern, ISACA released a light version of COBIT - called "COBIT Quick Start" which is considered a special version of COBIT that can be used as a baseline for many small to medium enterprises (SMEs) and other entities where IT is not mission-critical or essential for survival. It can also serve as a starting point for enterprises in their move towards an appropriate level of control and governance of IT [32].

ISO implementations are recognized especially in the financial sector driven by regulators compliance requirements. ISO 27001 is specifically used to establish ISMS. Its direct extension, ISO 27002, comes as a second step where detailed controls are needed. Based on our experience, we find ISO 27001 and ISO 27002 the easiest to automate and use for information security policies development and for conducting automated information security risk assessments. However, several organizations that pursue ISO certifications target marketing gains and overlook the fact that being certified does not necessarily means that you are secure. If not properly managed, ISMS certifications might lead to a false sense of security. On the other side, ISO 27005

which focuses on risk management is not a step by step risk assessment methodology compared to OCTAVE, but yet can be customized and used for this purpose and provide qualitative or quantitative security risk assessments.

ISO 27000 series implementation in general requires consultancy support that would bring cumulative implementation experience into action which would result in better results. ISO consultancy services are increasing on a sound base which is realized in offerings provided by the firms working in this area.

The concept of IT management as a service is the core of ITIL which came as a result of the increased dependence on IT and accordingly required more focus on high quality. Among the business drivers for ITIL implementation is the need for mature, well performing IT processes improvement of the quality of services, and considering IT users as service customers. ITIL can be used indirectly to achieve proper governance and risk management. Similar to COBIT, ITIL is process-based which facilitates its adoption and implementation by allowing focus groups to build it gradually. Despite its high adoption costs, ITIL is highly recommended for enterprises that have large IT back-office operations that support critical business operations. PCI DSS & Basel II are considered exceptional standards since their adoption is mandated by regulators and closely monitored for performance and possible weaknesses. However, having them fully implemented would reflect higher understanding of security requirements and would improve enterprises immunity against external and internal threats.

The OCTAVE methods have several important characteristics such as easy to execute and do not require large teams or advanced technical knowledge. They are also flexible and can be customized to address an organization's particular risk environment, security needs and level of skill. Also, risks are addressed in business contexts providing easy to understand results. It can be used also as the foundation risk-assessment component or process for other risk methodologies in a "hybrid-risk assessment" approach. OCTAVE information security risk assessments covers all information security aspects being physical, technical or people. A drawback in OCTAVE's various models is that they employ qualitative methodology only as opposed to quantitative approaches. Table 1 presents a detailed comparison matrix between the previously discussed standards.

7. Selection Process and Considerations

Based on the analysis presented in the previous sections, we found that various existing frameworks and standards have many strengths and weaknesses that promote or limit their adoption. The question of "which is the best" is a reasonable question to ask and we try to answer it in this section. Organizations should understand two key issues in order to be able to select an appropriate approach: understand the business objectives and requirements and understand the existing frameworks.

The answer to the above question depends heavily on understanding enterprises requirements and specific needs. If the exercise of requirements and needs analysis is not done, the adoption of a common standard just because it is widely used may be appropriate in some cases, and may be excessive or insufficient in others. The solution in this case is not a one size fits all solution and the decision to invest in implementing a certain standard should be carefully considered [16]. The expectation that one standard will fully address enterprises needs is not reasonable as it is difficult to develop a generic high level document that applies to all firms. We found no such study that promotes a specific standard as a solution for all issues related to information security risk management. This is where a customized-approach could actually be the best fit solution. A customized solution builds on the expertise of personnel and takes it into an aligned solution that matches enterprise requirements. Instead of using suggested content provided by the standards, the firm can build its own inventories of threats, vulnerabilities, and risks specific to its business type. Associated controls and control objectives need also to be customized based on the firm's objectives and risk appetite. A research conducted by GAO [11] detailed four case studies on information security risk assessment that show the

added value of a customized approach in addressing information security risk management issues. Locally developed customized approaches tend to mature and evolve over time and maintain close alignment with enterprise needs.

Another approach to use is the hybrid-approach which differs slightly from a customized-approach as it considers adopting more than one standard or framework to use on the bases of selecting which parts achieve the enterprise risk management objectives. For instance, an enterprise might select to adopt ISO 27001 for its ISMS organization structure and use OCTAVE as a risk assessment methodology. To build a comprehensive inventory of controls, COBIT might be selected for use, etc.

Understanding existing frameworks is the second key issue in selecting an appropriate standard. Before investing in the implementation of any specific framework or standard, it is imperative to make sure that those responsible for selecting a standard understand the exact characteristics of the standard in hand, what it is designed for, and accordingly can provide an initial estimate on its adequacy. Using case studies, benchmarking, and previous credentials the enterprise can have better understanding of the extent to which the selected standard would actually achieve the desired results. Because information security is becoming increasingly realized as a business issue, the selection team should include a knowledgeable business representative. This team member is expected to be aware of all compliance or regulatory requirements that the selected framework should address.

Once the business needs are specified and the available standards are explored, several other important factors should be considered in order to select a framework to use. These factors include:

Business nature: this includes the business sector (financial, health, government, etc.) and size. The type of threats, vulnerabilities, and risks associated with financial institutions are not the same for telecom operators or hospitals. Accordingly, the information security risk assessment requirements would vary from business to business and these are addressed differently in the standards. The enterprise size has a direct relation to what standard to adopt. SMEs might consider adopting standards or frameworks that have light weight versions. Many standards such as ISO 27001 do not have light versions [7].

- *Cost of implementation:* this factor can be considered a differentiator in situations where more than one standard or framework fulfills the enterprise needs and the cost of their implementation is different. Usually such implementations are executed through consultants or third parties who have specific fees for their services; however, this is not the only expense to account for. Project management, required organizational changes and resources (awareness programs), day-to-day operation to maintain compliance with the implemented standard are some other expenses to mention [7].
- *Needed skills:* the needed skills to implement and operate an information security management are not the same for all frameworks. Some frameworks require business knowledge, project management and budgeting skills where some other standards require more technical skills. PCI DSS for instance requires more technical knowledge than ISO 27001 or COBIT which focus more on business understanding.
- *Generality:* when selecting a framework to use for information security risk assessment, it is quite important to recognize whether the framework being inspected provides the needed details and how-to or it just covers the topic in general. Comprehensiveness is another aspect to inspect as well, which indicates the degree of coverage provided by the framework. ISO 27001 is a general standard to use for information security risk management contrary to ISO 27005 which is specific to security risk management. ISO 27002 does not provide a comprehensive inventory of all controls to implement [7, 31].
- *Adoption by other enterprises:* adoption by others can act as a main indicator that assists enterprises in selecting a standard or framework that best fits into their needs, especially if used to provide a benchmark that compares to similar implementations in similar businesses. ISACA for instance publishes case studies on COBIT's implementation that detail why COBIT was

used and how it assisted in addressing enterprises requirements [31].

- *Availability of detailed guidelines from owner:* this aspect is important especially if the enterprise decided to implement the standards or frameworks depending on its own resources without the assistance of a third party or external consultant. However, not all standards have detailed guidelines from the owners.
- *Implementation complexity:* a standard that meets the enterprise requirements and is yet simple to implement is considered a better option. In some cases, a standard that looks theoretically appropriate may have a very complex implementation. This issue might be standard-neutral, however, it reflects on the overall framework adoption [7]. The implementation complexity can be measured in terms of the number of teams that need to be involved, estimated changes to be introduced to existing processes or operations, etc.
- *Flexibility and customization:* a key feature that should be considered in selecting a standard for adoption is its flexibility and ability to be customized. This assists in implementing a customized-approach based on the enterprise needs. Customization is usually done to aid the development of an automated solution for the assessment.
- *Others:* the existence of suggested or proposed controls and control objectives inventories, compliance mandatory or not, is there a certification to acquire after implementation, availability of ready to use automated tools and multi-language support.

8. Suggested Approach and Recommendations

In order to assist in the resolution of the problem resulting from the existence of multiple information security risk management frameworks and standards, we propose a selection model based on the Simon decision making model [33]. According to Simon, there are four different stages in decision-making: intelligence, design, choice, and implementation. Intelligence relates to the identification of the problem that needs to be solved. This requires the individual problem solver to gather information about the area under scrutiny. Design refers to the alternative solutions that the individual problem solver considers to solve the identified problem. This stage often requires obtaining additional information beyond what was collected during the intelligence stage. Choice consists of choosing among the various alternative solutions identified in the design stage. This stage may also require obtaining additional information beyond what was collected during the intelligence and design stages. Implementation relates to the execution of the solution choice made in the previous stage. It also includes the continuous reporting on the progress of the chosen solution.

Whereas Simon's model is a general model of decision making, we feel it is appropriate when considering selecting an information security standard because the latter is a major decision that an organization makes. However, because Simon's model is a general model of decision-making, not specific to standard selection, it needs to be adapted. From an analysis of the information gathered during the case study discussed in the next section and based on our practical experience with our clients, we developed a selection process that parallels the decision-making process an enterprise goes through when evaluating its standards' options and subsequent outcomes. Figure 1 shows how we started with Simon's four-stage model of decision-making, and then adapted it to 5 stages to better reflect what we thought should occur when enterprises evaluate and address information security risks. This part of our process is depicted as Framework Selection Stages. Stage 1 - why is similar to Simon's intelligence where the enterprise weighs up the advantages and disadvantages of considering an information security framework/standard. Stage 2 - what is similar to Simon's design where the enterprise addresses what alternative framework arrangements are to be considered and which might be most appropriate. Stage 3 - which is similar to Simon's choice that reflects the actual decision made by the enterprise when comparing and shortlisting the various options. These three stages are combined to form what we consider the first phase of the framework selection process: the

Decision Phase. Stage 4 - how is consistent with Simon's implementation where the enterprise chooses a security framework from the shortlist produced in the previous stage, or selects a combination of frameworks, and implements metrics to evaluate the selected option. Stage 5 - outcomes reflects the consequences of making the security framework choice; the success or failure of the arrangement, and the lessons learned. We combine these two stages into a second phase of the framework selection process, which we refer to as the Implementation Phase. These stages are further expanded to include the activities that enterprises go through as they progress their framework selection and evaluation. This is depicted in the figure as Application of Framework Selection stages.

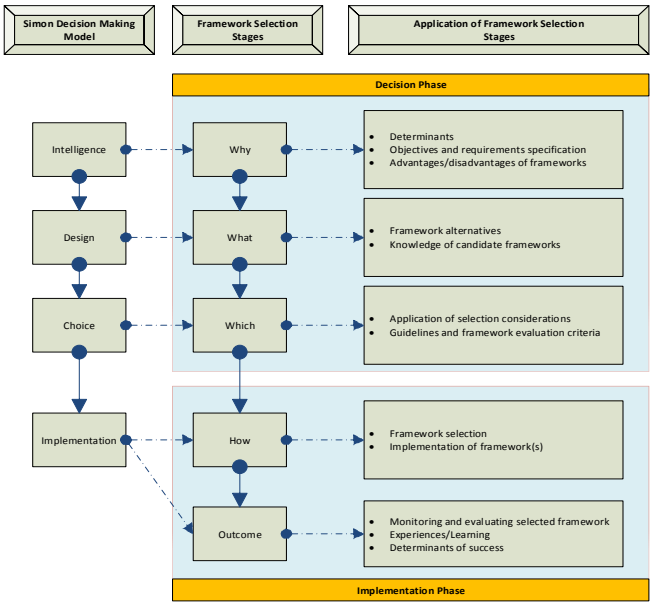

Fig. 1. Proposed Model for Framework Selection.

According to the model, we begin by asking why an enterprise might consider using a security standard to address security risks. What are the conditions or situations (i.e., the determinants) that might lend themselves to a decision to use a standard/framework? What are the advantages and disadvantages associated with using or not using a security standard? To answer these questions, the enterprise should clearly understand the requirements and the objectives to be achieved.

One can argue that the question of what kind of security framework to consider (information, services, infrastructure, etc.), to address associated security risks, can only be answered if two conditions are fulfilled. First, at least two different options have to be available. Second, there needs to be a reason or a rationale that serves as a selection criterion. The latter is related to the question "why use a standard to protect against security risks". In fact, the answers to "why use a standard" can be used as criteria to evaluate the options available when asking "what type of framework".

After considering what framework type to use, the next question faced is 'which choice to make'. In making the choice to use a security standard, enterprises should understand the details of the candidate frameworks in order to arrive at a selection decision; guidelines to help them assess the various selection criteria and their choice should be specified. The enterprise should create a shortlist of potential frameworks, combinations of frameworks (hybrid approach), or a customized framework. Here, the selection considerations recommended in this article can be used as guidance.

After answering the preceding questions, the enterprise is faced with a host of implementation decisions, which can be summarized by asking 'how to implement a successful and effective security framework'. In considering 'how', we focus on framework implementation. This includes three issues: selecting a framework, a customized or a hybrid solution; implementing or outsourcing the implementation of the framework; and specifying metrics to evaluate the effectiveness of the selected framework. In general, 'how' relates to the implementation of best practices – methods, techniques, and approaches used to effect the framework selection decision that tend to result in a higher degree of information security risks management success (i.e. outcome).

After, and even during, the implementation of a security framework, enterprises must look at the results of their framework choice. That is, they must evaluate the actual 'outcomes' of the framework implementation. What are the experiences of enterprises that have implemented a security framework? What lessons learned might we glean from them? How could they lead to enterprise success? What implications do they have for the practice of information security risks

management? Thus outcomes deal with the wider implications of framework selection decisions.

Based on our analysis and research, we put forward some recommendations that we believe when adopted and implemented properly, can add value and consolidate the efforts for advancing this field:

- *Spend more efforts to understand existing standards & frameworks:* More efforts should be spent in order to reach comprehensive understanding of the existing information security frameworks and standards. This will assist in building a systematic approach for selecting the best for the enterprise in addition to making it easier to implement and eliminate possible complexities and weaknesses. Deep understanding will be of a unique value when the enterprise decides to customize a framework to fit into its specific needs.
- *Maintain consistency:* Whether the enterprise decided to adopt a standard as is or wanted to have it customized, the information security risk management program must maintain consistency for all aspects. This is imperative especially when implementing customized or hybrid approaches where the need for making sure that no conflicts exist is important. If consistency is not maintained conflicts might result into waste of time, efforts and resources.
- *Build local competencies:* Enterprises should consider investing in leveraging staff competencies in information security risk assessment. This can be in the form of continuous awareness sessions, training and motivating staff to complete education or acquire degrees in related fields. It is important to notice that the competency needed is not limited to technical knowledge but includes project management and analytical skills as well.

9. Case Study

Case studies are appropriate for exploratory and explanatory research, since they are able to capture a greater depth and breadth of detail on the subject's activities. They are particularly powerful techniques to answer "how" and "why" questions, and offer rich insight. The strength of the case study is also in its use for examining natural situations and in the opportunity it provides for deep and comprehensive analysis.

The key objective of the case study used in this research is to support the proposed model findings and provide additional evidence through comparing theory with practice in the field of information security risk management. The purpose of this case study is thus to show how the suggested approach can benefit organizations in addressing their technology and information security risks. The case study is related to one of the largest banks in Jordan, namely Al-Ahli Bank that relies heavily on the use of technology. The bank wanted to leverage the maturity of its IT processes and conduct a detailed risk assessment for the existing processes in addition to suggesting areas of improvement. The organization management believed that becoming ISO 27001 certified will address their requirements. The major driver behind their selection for ISO 27001 was "Increasing Marketability". We applied our five step approach and started the engagement with a detailed current state assessment. The understanding was done through one to one meetings, questionnaires and group discussions. According to the conducted understanding, the initial requirements were tuned and discussed with management in order to specifically identify detailed objectives to target. We realized that both the IT and the information security entities were not mature and needed improvement. We discussed with management that trying to apply ISO 27001 blindly, in the absence of proper foundations, would not add value to the firm. Based on our detailed understanding of the existing frameworks, the results of the gap analyses conducted, as well as using our proposed model, we decided to use the "Hybrid" approach. We agreed to use ISO 27001 to establish the information security entity. This included mainly the development of all missing policies, processes, and procedures. The ISO 27005 was used to conduct the IT risk assessment utilizing the detailed list of controls and control objectives from ISO 27002. To properly establish the IT entity, COBIT was used. COBIT, which focuses on IT

governance and alignment of all IT activities with business objectives, was well accepted by the firm's management.

Initially, the company strongly believed that ISO 27001 ISMS implementation would address their IT and information security risks. However, when we applied our five-step approach it turned out that a combination of standards would better satisfy the needs of the company and was of more added value. We provided detailed understanding of what ISMS could provide, and based on the firm's real needs we used different frameworks effectively to achieve the desired objectives. The ISMS was used only to establish the information security organization where risk assessment was based mainly on ISO27005. The use of COBIT provided comprehensive evaluation for their IT entity which cannot be separated from the security entity but yet won't be covered or evaluated while using ISMS. Highlighting the importance of aligning IT objectives with business objectives along with providing detailed understanding of the current IT processes effectiveness gave the organization much more than what ISMS alone could do.

As a result, our approach has changed the organization focus from increasing marketability to establishing well structured and healthy IT and information security entities that would eventually assist the firm in achieving its business objectives and strategic goals.

10. Conclusion and Future Work

Risks associated with the use of technology need to be properly managed and assessed in order for enterprises to maintain their businesses. Some of the challenges that hinder IT risk assessments were discussed in this paper. In response to these challenges, enterprises tend to adopt leading market practices and standards to assist in conducting consistent assessments. However, the existence of many frameworks and standards adds to the ambiguity and raises the concern of which is better. This paper discussed the most common frameworks used in information security management, namely COBIT, ITIL, Risk IT, ISO 27001, ISO 27002, ISO 27005, Basel II, PCI DSS and OCTAVE Set. Strengths and weaknesses of these frameworks were discussed. Based on our research and experience, we proposed a selection model along with a suggested process for IT risk management. The successful implementation of the proposed solution will contribute to a holistic approach to IT risk management. As a proof of concept, the proposed approach has been applied using a real-life case study, which has proved its adequacy and usefulness.

References

[1] Symantec, "Symantec Global Internet Security Threat Report Trends for 2008", *Symantec's Publications,* Vol. XIV, 2009, pp. 10.

[2] www.gocsi.com, "Computer Crime and Security Survey", accessed January 2012.

[3] B., Blakley, E., McDermott, and D., Geer, "Information Security is Information Risk Management", *ACM Digital Library*, 2002.

[4] E., Humphreys, "Information security management standards: Compliance, governance and risk management", *Information Security Technical Report*, Vol. 13, No. 4, 2008.

[5] H., Susanto, M., Almunawar, and Y. Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five", *International Journal of Electrical & Computer Sciences*, Vol. 11, No. 5, 2011.

[6] Y., Barlette and V., Fomin, *The Adoption of Information Security Management Standards: A Literature Review*, IGI Global, 2009.

[7] S., Schlarman, "Selecting an IT Control Framework", *EDPACS*, Vol. 35, No. 2, 2007.

[8] , J., Sipiorand and B., Ward, "A Framework for Information Security Management Based on Guiding Standards", *Issues in Informing Science and Information Technology*, Vol. 5, 2008.

[9] A., Tsohou, S., Kokolakis, C., Lambrinoudakis, and S., Gritzalis, "A security standards' framework to facilitate best practices' awareness and conformity", *Information Management & Computer Security*, Vol. 18, No. 5, 2010, pp.350 – 365.

[10] A., Calder and S., Watk, *IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002*, Kogan Page Limited, UK, 2008.

[11] Government Accountability Office (GAO), *Information Security Risk Assessment: Practices of Leading Organizations*, GAO Publications, 1999.

[12] IT Governance Institute (ITGI), *COBIT 4.1* (1st edition), ITGI Publication, United States, 2007.

[13] International Standards Organization (ISO), *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO/IEC Publications, Switzerland, 2005.

[14] L., Coles-Kemp and R., Overill, "The Information Security Ownership Question in ISO/IEC 27001 – an Implementation Perspective", *4th Australian Information Security Management Conference*, 2006.

[15] www.raa.si, "Risk Tools Matrix", accessed January 2012.

[16] K., Brotby, Information Security Governance: *A Practical Development and Implementation Approach*, Willy & Sons/New Jersey, 2009.

[17] International Standards Organization (ISO), *Information Technology – Security Techniques – Code of Practice for Information Security Management*, ISO/IEC Publications/ Switzerland, 2005

[18] The Open Group, *ISO/IEC 27005 Cookbook*, Open Group/UK, 2010.

[19] searchcompliance.techtarget.com, "Compliance Topics", accessed January 2012.

[20] International Standards Organization (ISO), *Information Technology – Security Techniques –Information Security Risk Management*, ISO/IEC Publications/Switzerland, 2008.

[21] Office of Government Commerce (OGC), *Passing Your ITIL Foundation Exam*, OGC Publication/UK, 2007.

[22] N., Bruton, *The ITIL Experiance: Has it been Worth it?*, Bruton Publications, 2004.

[23] A., Cater-Steel, W., Tan, and M., Toleman, "Summary of ITIL Adoption Survey Responses", *itSMF Australia 2006 Conference*, 2006.

[24] Hornbill Systems: "ITIL: *State of the Nation Survey Findings*, Hornbill Systems Publications, 2009.

[25] www.isaca.org, "COBIT 4.1 Case Studies", accessed January 2012.

[26] Information Systems Audit & Controls Association (ISACA), *Risk IT Framework*, ISACA Publication/United States, 2009.

[27] www.bis.org, "Basel II", accessed January 2012.

[28] Information Systems Audit & Controls Association (ISACA), *IT Control Objectives for Basel II: the Importance of Governance and Risk Management for Compliance*, ISACA Publication/ United States, 2007.

[29] Payment Card Industry Council (PCI-Council), *PCI DSS 2.0*, PCI Council Publication/United States, 2010.

[30] Software Engineering Institute (SEI), *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, SEI Publication, 2007.

[31] K.J., Knappeat, *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, IGI Global/United States, pp 119-140, 2009.

[32] IT Governance Institute (ITGI), *COBIT 4.1 Quick Start*, ITGI Publication/United States, 2007.

[33] H. A., Simon, *The New Science of Management Decision*, Harper/New York, 1960.

Table 1. Standards Comparison Matrix

GRC DOC	H[1]	H[2]	H[3]	H[4]	H[5]	H[6]	H[7]	H[8]	H[9]	H[10]	H[11]	H[12]	H[13]	H[14]	H[15]	H[16]	H[17]	H[18]	H[19]	H[20]	H[21]
ISO 27001	S	H	A	Y	G	N	N	Y	ISMS	N	Y	H	H	Y	Y	N	N	N	Y	Y	D
ISO 27002	S	H	A	Y	G	N	N	Y	COP	N	Y	H	H	Y	Y	N	N	N	Y	Y	D
ISO 27005	S	H	A	Y	S	Y	N	Y	ISRM	N	Y	H	H	Y	N	N	N	N	N	Y	D
COBIT 4.1	F	H	A	Y	G	Y	Y	Y	ITG	Y	Y	H	H	Y	Y	N	Y	N	N	Y	D
ITIL 3.0	F	H	A	Y	G	Y	N	Y	ITSM	N	Y	H	H	Y	N	N	Y	N	N	Y	I
RISK IT	F	H	A	Y	S	Y	N	Y	ITRM	N	Y	H	H	Y	N	N	Y	N	N	Y	D
Basel II	R	M	M	N	G	N	N	Y	OPR M	N	Y	M	L	Y	N	Y	N	Y	N	Y	I
PCI DSS	S	H	A	Y	G	Y	N	Y	CDS	N	Y	H	L	Y	Y	Y	N	Y	Y	Y	D
OCTAVE Allegro	M	M	M	Y	S	Y	N	Y	ISRD	Y	Y	L	M	Y	N	N	N	N	N	Y	D
OCTAVE	M	L	S	N	S	N	Y	N	ISRD	N	Y	L	M	Y	N	N	N	N	N	Y	D
OCTAVE –S	M	L	S	N	S	N	Y	N	ISRD	N	Y	L	M	Y	N	N	N	N	N	Y	D

[1]Category: **F**ramework, **S**tandard, **R**egulation, **M**ethodology
[2]Cost of Implementation: **H**igh, **M**edium, **L**ow
[3]Needed Skill Level: **A**dvanced, **M**oderate, **S**imple
[4]Advisory Consultancy Needed: **Y**es, **N**o
[5]Generality (multipurpose): **G**eneral, **S**pecific
[6]Comprehensive (provides full coverage): **Y**es, **N**o
[7]Suitable for SMEs: **Y**es, **N**o
[8]Suitable for Large Firms: **Y**es, **N**o
[9]Main Purpose: **ISMS** (Information Management System), **ISRM** (Information Security Risk Management), **ITG** (IT Governance), **ITRM** (IT Risk Management), **ISRD** (Information Security Risk Methodology), **CDS** (Card Data Security), COP (Code of Practice), **OPRM** (Operations Risk Management), **ITSM** (IT Service Management)
[10]Existence of Light Version: **Y**es, **N**o
[11]Availability of Detailed Guidelines from Owner: **Y**es, **N**o
[12]Implementation Complexity: **H**igh, **M**edium, **L**ow
[13]Flexibility & Customization**:** **H**igh, **M**edium, **L**ow
[14]Implementation Measurement Automation: **Y**es, **N**o
[15]Suggests Controls & Controls Objectives: **Y**es, **N**o
[16]Industry Specific: **Y**es, **N**o
[17]Implementation on per Domain-basis: **Y**es, **N**o
[18]Compliance Mandated: **Y**es, **N**o
[19]Certification Possibility: **Y**es, **N**o
[20]Availability of Tools: **Y**es, **N**o
[21]Kind of Support: **D**irect, **I**ndirect