Guide to ISO 27001: UAE Case Study

Manar Abu Talib
Zayed University,
Abu Dhabi, UAE
manar.abutalib@zu.ac.ae

May El Barachi
Zayed University,
Abu Dhabi, UAE
may.elbarachi@zu.ac.ae

Adel Khelifi
ALHOSN,
Abu Dhabi, UAE
a.khelifi@alhosnu.ae

Olga Ormandjieva
Concordia University,
Montreal, Canada
ormandj@cse.concordia.ca

Abstract

ISO/IEC 27001 is the most used standard within the information security field. It is used by organizations that manage information on behalf of others and it is applied to assure the protection of critical client information. In general, applying ISO standards could be costly and require expert people. This paper introduces a survey study about using the standards in the UAE and details three case studies on ISO 27001 implementation: One case study follows the ISO 27001 framework, and it is expanded by using additional management processes. The second case study integrates both ISO 27001 and ISO 20000 standards. The final case study details the certification process for ISO 27001 only. This research paper shows that the use of ISO 27001 in this region of the world is quite promising and puts the guidelines for any organization interested to apply this standard..

Keywords: Information Security, ISO/IEC 27001, survey, case study, ISO 20000.

Introduction

The United Arab Emirates (UAE) and the other Gulf countries are working together to harmonize their standards since standards ensure a high level of quality, safety, reliability, and efficiency in the products and services they all use (Richards & Dar, 2009). The best known standards organizations are: the International Organization of Legal Metrology (OIML) in Paris [http://www.oiml.org/]; the International Organization for Standardization (ISO) in Switzerland [http://www.iso.org/iso/home.html]; the International Electro-technical Commission (IEC) in Switzerland [http://www.iec.ch/]; the Institute of Electrical and Electronics Engineers (IEEE) in the USA [http://www.ieee.org/index.html]; and the International Telecommunication Union (ITU) in Switzerland [http://www.itu.int/en/pages/default.aspx].

Around 162 countries apply ISO standards since the International Organization for Standardization (ISO) has variety of 17,500 international standards,

1,100 new standards being established every year (ISO, 2010). ISO/IEC 27001 is the most used standard within the information security field. It is used by organizations in order to handle information safely and securely; and to audit the accuracy, confidentiality, and integrity of information within an organization (ISO/IEC 27001, 2005; ISO/IEC 27002, 2005; ISO/IEC 27002, 2005; ISO/IEC 27006, 2005).

Although ISO IT standards could be directly implemented by many companies and taught in some universities in the UAE, this kind of data must be collected and provided to the Emirates Authority for Standardization and Metrology (ESMA) (2010) in order for this organization to officially adopt them. Our objectives in this paper are the same ones published in the previous work (Abu Talib, Khelifi, & El Barachi, 2011), which are: 1) Increase the freedom of choice of IT security techniques; 2) Increase the extent of usage of ISO standards in the IT field; 3) Reduce the gap between ESMA and both industry and academia (i.e. companies and universities); and 4) Update the document entitled "Standardization & Classification in the UAE," previously published by Al Tamimi & Company, which currently lacks information about ISO IT standards. One more objective is to put the guidelines for any organization interested to apply ISO 27001 standard through introducing three detailed case studies. In future research, we aim to study about the possibility of integrating ISO standards to IT curriculums in order to produce graduates that have the knowledge needed by the market place.

The rest of the paper is organized as follows. In the next section, we present background information on IT standards in the UAE. The method and experimental setup used in our research survey are introduced in the third section, followed by presentation and analysis of the results obtained in the fourth section. In the fifth section, we present three case studies on ISO 27001 use in the UAE. In the final section, we provide our conclusions and an outline of future research directions.

IT Standards in the UAE

In 2001, ESMA was established as a federal UAE Authority, as a result of UAE Federal Law No. 28. ESMA's main goal is to improve the national economy and help promote standards of excellence and quality in the UAE. Of 17,000 international standards, more than 1,800 of them are being implemented in the UAE through ESMA. All these standards are used to develop the UAE economy and improve its status within the global economy. ESMA's main goals are: to achieve health care security, economic security, and environmental security; to support the national economy; to become up to date with the progress of scientific and quality control standards and to provide education on standardization and information on metrology activities (ESMA, 2010).

Specifically, ESMA seeks to focus its efforts on the IT field, targeting such areas as: 1) information technology for learning, education, and training; 2) IT security; 3) office equipment; 4) identity cards and other modes of personal identification; and 5) software and systems engineering.

We conducted several meetings with ESMA to help them in collecting some data about the IT ISO standards used in the UAE. The first survey was distributed to sixty-four organizations in the UAE (January 2010 to April 2010) (Abu Talib et al., 2011). We found that 8% of the surveyed organizations are ISO 27001 certified, while 92% are not. The certified organizations have followed many international standards over the years with the help of experts from different parts of the world. These standards were implemented because they are well known, well crafted and highly effective. We should also mention that, although a large number of the organizations surveyed are not certified, they apply their own procedures and policies that are derived from international standards. Overall, there is a high level of awareness of security standards in the UAE, and even non certified organizations are familiar with many of them, ISO 27001 (Information Security Management Systems Requirements) being the most popular and most widely applied in this country. Small organizations, by contrast, and the most recently established ones, will focus

on other things than ISO certification, such as gaining market share and realizing profit (Abu Talib et al., 2011).

In this study, we have started the research by a general survey study in order to explore in greater detail the broad applicability of IT standards in different sectors, study the advantages and disadvantages of using them and to investigate the future need of organizations for IT standards. Since ISO 27001 is the most popular standard in the UAE, three case studies have been detailed in three different contexts. At the end of this study, we provided an overview of using IT Standards in the UAE, guidelines of how to apply ISO 27001 and the lessons learnt from ISO 27001 implementation. Our research framework is detailed in Figure 1.

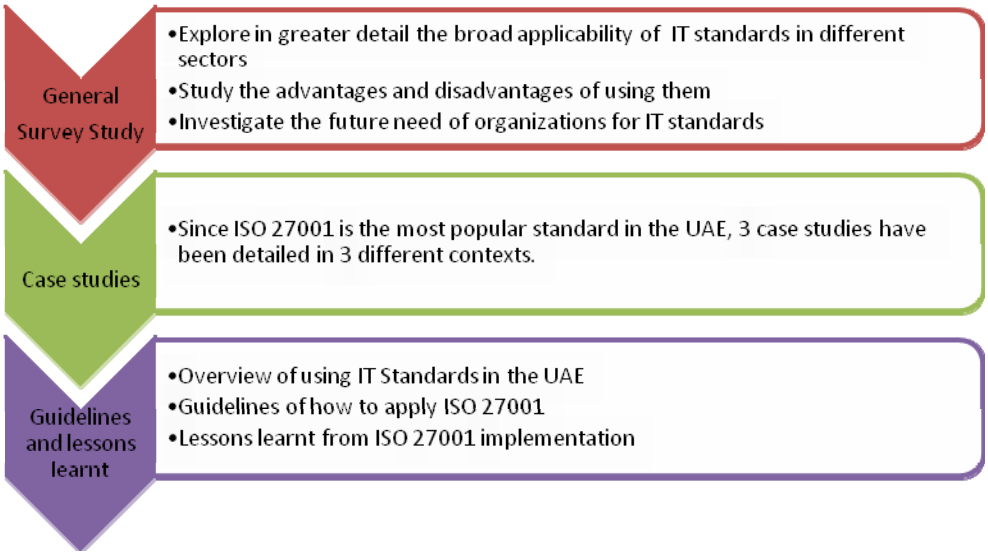

Figure 1: The methodology used in this study

Research Method and Experimental Setup

To measure and evaluate the use of ISO security standards in UAE organizations, we chose one of the most popular empirical investigation methods – the survey. The reasons behind our choice of empirical investigation approach are as follows: i) the investigation of the impact of ISO security standards in UAE organizations is retrospective: ii) we have no control over the activity that is under study, that is, the adoption of an ISO standard by an organization, and iii) the research was conducted on large scale (Fenton & Bieman, in press). An online survey was created using the SelectSurvey tool, and a printed version was sent to participants who could not fill it out online. SelectSurvey tool is a Web-based survey application available for faculty and staff at Zayed University to enable the collection of data relating to research, business, and academic needs.

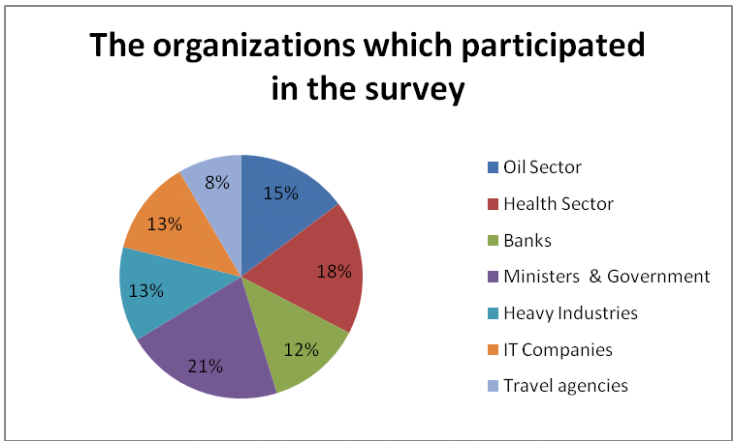

Figure 2: Categories of survey participants. ("Organizations participating in the survey"; "Oil"; "Health"; "Ministries & government"; "Heavy industry"; "IT"; "Travel agencies")

The survey was distributed among 95 organizations in the UAE (September 2010 to December 2010). These organizations belong to seven different sectors: oil, health, banking, ministries & government, heavy industry, IT, and travel agencies. The chart below indicates the percentage of organizations participating in the survey:

The responses to the survey indicated that there is a high level of awareness about IT standards usage. For example, large organizations usually give a high value to meeting quality standards, and are prepared to invest in implementing some international standards. Applying these standards in an organization takes a long time and requires a significant amount of work, people, and experience, however, not every organization can afford to do so. In fact, large organizations and government organizations are the most likely to apply international standards. Because these organizations have a sizeable market share, they have a significant influence in the marketplace. As a result, implementing or following international standards emerges as a competitive advantage, and will intensify the competition between them. Examples of ISO certified organizations are: Abu Dhabi Gas Industries Ltd. (GASCO) and Advanced 4C Solutions Company (ISO 27001 and ISO 9001), Injazat Data Systems (ISO 27001 and ISO 20000), and the Ministry of Finance and the Finance House (ISO 27001). Some organizations, like the Cornish Hospital and Abu Dhabi Systems and Information Centre (ADSIC), follow the framework of the security standards. The Cornish Hospital is also willing to become EIA and COBIT certified. Others are merely aware of the IT standards. Figure 3 illustrates their wide applicability.

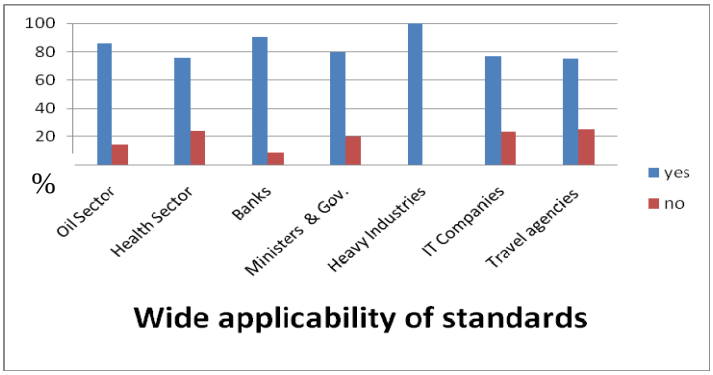

Figure 3: Wide applicability of IT standards. ("Oil"; "Health"; "Banking"; "Ministries & government"; "Heavy industry"; "IT"; "Travel agencies")

Part I: Organizations that apply IT standards

The survey has revealed the most frequently cited advantages and disadvantages of using IT standards. These are listed in the table below.

Table 1 Advantages and Disadvantages of Using IT Standards in the UAE

Advantages	Disadvantages
- Benefits to businesses - Common understanding - Best practices, state of the art - Protection of businesses - Technical agreements - Interoperability - Worldwide technology compatibility - Efficiency and customer satisfaction - Requires commitment - System stability, easy to upgrade - Global recognition of product quality - Skills enrichment and risk avoidance	- Expensive, requires specific IT budget - Special expertise required - Lack of knowledge - Not easy to use - Time required to apply them to organizational users - Resources required to provide ongoing training and awareness

Table 2 shows that organizations use different international standards (including IT standards and non IT standards), model standards, open standards, platforms and common frameworks mainly based on sector needs, and on improving efficiency and customer satisfaction. For example, the international standards most often used by banks are ISO 27001 (Information Security) and ISO 9001 (Quality Management System).

Table 2 Examples of Standards Used in Various Sectors in the UAE

Sectors	Oil	Health	Banking	Ministries & government	Heavy industry	IT	Travel Agencies
Standards used	ISO 27001	ISO 27000	ISO 9001	ITIL	IEEE 802	COBIT	SAP
	ISO 9001	ISO 20000	ISO 27001	ISO 27000	ISO/ICE 9126	CMMI*	
	ISO 9000	ISO 9000	ISO 38500	ISO 20000	ISO 9001	PMI*	
	IEEE 802	TIA*	ISO 20000	ISO 27001	ISO 9002	MSF*	
	ITIL*	JCI*	IEEE 802	ISO 9001	ISO 14001	ITIL	
	ITIL V3	SKEA*	COBIT	ISO 9000	ISO/IEC 13567	IEEE 802	
	MS	ACHS*	CISA*	IEEE 802		PCL*	
	HSE	HAAD*	Prince 2*	IAEA*		J2EE*	
		IEEE 802	ITIL	ADSIC			
		EIA		ITIL V2			
		ITIL		BPMN*			
		COBIT*		SOAP*			
				RDF*			
				SOAP			

Acronyms

ITIL: an integrated set of best practice lifecycle recommendations with common definitions and terminology (Information Technology Infrastructure Library, 2007).

TIA: accreditation by the American National Standards Institute (ANSI) to develop voluntary industry standards for a wide variety of telecommunications products (Telecommunications Industry Association, 2011).

JCI: an accreditation organization dedicated to improving the safety and quality of health care in the international community through the provision of education, publications, consultation, and evaluation services (Timmons, 2003).

SKEA: Sheikh Khalifa Excellence Award, to provide organizations with a road map to help them improve their performance, to support a healthy economy, and to unify their management practices in a balanced, holistic model: http://www.skea.ae .

ACHS: an independent organization dedicated to improving the quality of health care through continual review of performance, assessment and accreditation (Australian Council on Healthcare Standards, 2011).

HAAD: Health Authority – Abu Dhabi (http://www.haad.ae , the authority responsible for regulating all aspects of health care provision, including quality of care and patient safety. Their standard for the diagnosis, management, and data reporting for diabetes applies to all the health care facilities and professionals they license, and is also intended to ensure that patients with diabetes mellitus receive safe, quality care.

COBIT: an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks. It enables development of clear policies and good practices for IT control throughout organizations, emphasizes regulatory compliance, helps organizations increase the value attained from IT, enables alignment of the COBIT framework, and simplifies its implementation (Information Systems Audit and Control Association, 2011).

IAEA: Three main areas of work; Safety and Security; Science and Technology; and Safeguards and Verification (International Atomic Energy Agency, 2011).

PRINCE2: PRojects IN Controlled Environments (http://www.prince2.com/what-is-prince2.asp), a process-based method for effective project management. It is a de facto standard used extensively by the UK Government, and widely recognized and used in the private sector, both in the UK and internationally.

BPMN: Business Process Modeling Notation, a standard for business process modeling, providing a graphical notation for specifying business processes in a Business Process Diagram (BPD), based on a flowcharting technique very similar to Unified Modeling Language (UML) activity diagrams (Hommes & Hommes, 2004).

SOAP: a simple and open standard XML-based protocol for exchanging information between computers.

RDF: a standard model for data exchange on the Web. RDF has features that facilitate data merging even when the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed.

CMMI: Capability Maturity Model Integration, a model that consists of best practices for system and software development and maintenance (Software Engineering Institute, 2010).

PMI: Project Management Institute (http://www.pmi.org) offers a comprehensive certification program for project practitioners of all education and skill levels.

Microsoft Solutions Framework: MSF, a project management system that IT professionals use to manage large projects. The framework comes with a set of principles, business models, concepts and tools to help IT project managers plan and complete projects (Microsoft Solutions Framework Certification, 2011).

PCL: the standard print format for HP LaserJet-compatible printers

J2EE: Java 2 Platform, Enterprise Edition, defines the standard for developing multitier enterprise applications. The J2EE platform simplifies enterprise applications by basing them on standardized, modular components, by providing a complete set of services to those components, and by handling many details of application behavior automatically, without complex programming.

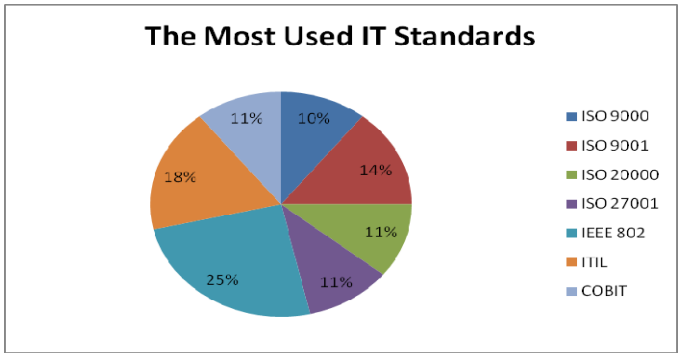

Figure 4: Examples of international standards based on sector needs. (IT Standards Most Commonly Used)

Based on the survey results, the standards most commonly used by organizations are:

1. IT security techniques: 65%.
2. Telecommunications and information exchange between systems: 44%.
3. Identity cards and personal identification: 39%.
4. Information technology for learning, education, and training: 38%.
5. Data exchange and management: 36%.

Part II: Organizations that do not apply IT standards

The table below shows the most commonly cited reason why organizations do not use IT standards:

Table 3 Reasons for Not Applying IT Standards in the UAE

Sectors	Oil	Health	Banking	Ministries & government	IT	Travel agencies
Why IT standards are not applied	Other alternatives available Not easy to use	Expensive Lack of knowledge Other alternatives available Plan to use them in the future	Having other alternatives Lack of knowledge	Special expertise required Expensive Lack of knowledge Plan to use them in the future	Other alternatives available	Other alternatives available Lack of knowledge

Based on the survey results, the IT standards needed most by these organizations are:

1. IT security techniques: 65%
2. Data exchange and management: 50%
3. New and emerging IT issues: 50%
4. IT for learning, education, and training: 42%
5. Software and system engineering: 42%.

ISO 27001 Certification in the UAE: Case Studies

In information security, ISO 27001 (known as the Information Security Management System (ISMS) standard) (ISO/IEC 27001, 2005) is the most widely used standard. It focuses on ensuring integrity, availability, and confidentiality, and is a recognized structured methodology dedicated to information security. ISO 27001 is described as a management process that can be used to evaluate, implement, and maintain an Information Security Management System (ISO/IEC 27001, 2005). Most companies around the world are working to apply this standard for many reasons, among them: reducing liability due to unimplemented or enforced policies and procedures; measuring the success of security controls; and improving the effectiveness of information security. In this section, we introduce three detailed case studies on the use of ISO 27001 in the UAE.

ADSIC Case Study

This case study details the start-up and growth of the Abu Dhabi Information Security Program, which has been implemented in many Abu Dhabi Government entities with the help of the Abu Dhabi Systems & Information Centre (ADSIC) (http://adsic.abudhabi.ae/Sites/ADSIC/Navigation/EN/root.html). It began as a committee item approved in October 2005 by Executive Council Decree No. 33, issued by HH Sheikh Mohammed bin Zayed Al Nahyan, Crown Prince of Abu Dhabi, Deputy Supreme Commander of the UAE Armed Forces and Chairman of the Abu Dhabi Executive Council.

Mr. Karmastaji, the Standards and the Governance Manager of ADSIC, talked about ADSIC's program, and how they came to follow the ISO 27001 framework based on the needs of UAE

government entities. This program is consistent with the ISO 27001 framework and expands on it using additional management processes (Abu Talib et al., 2011).

The Abu Dhabi Government has implemented a Risk Management Process through ADSIC, which aims to protect not only Information Technology (IT) assets, but also the business processes of all public entities across Abu Dhabi to ensure that the appropriate C.A.I is provided for all information. The Risk Management Process is an ongoing one, which is guided by the Plan-Do-Check-Act (PDAC) model to determine which controls are required, and basically to allow the implementation of the right security controls in order to address all risks. It comprises four main phases: Risk Assessment, Information Security Planning, Security Testing & Evaluation, and Certification & Accreditation (Figure 5).

Figure 5: Risk Management Phases

Guidelines for Following ISO 270001 Standard Without Certification:

Phase I: Risk Assessment. This phase is mandatory in the Risk Management Process, as it serves as the foundation for the other phases. Performing the Risk Assessment helped ADSIC identify weaknesses in government services and enabled the management team to make decisions regarding implementation of the security controls and the remediation measures. Risk Assessment promotes a consistent approach to measuring risks and allows stakeholders to place values on potential losses. There is a sequence of steps that must be implemented in order to complete this phase, including: scope definition, asset identification, impact assessment, and threat, vulnerability, and risk identification.

Phase II: Information Security Planning. The goal of the planning phase is to protect the information of Abu Dhabi Government entities from risk and the damage that can occur, such as unauthorized access to information, loss of information, and wrongful use or modification of information. It is an important step, because it helps address the risks that were identified in the Risk Assessment phase by reducing or avoiding them. This phase helps in selecting the controls that address the security risks, and in documenting the planned and implemented controls for the information system. Security issues must be addressed continually, which makes planning for information security an ongoing process. This phase is implemented by the system owner, the owner of the governance entity, for example, who is also responsible for implementing the security controls in that system. The time needed for this phase depends on the supporting systems and services. This is because less time is required to evaluate a simple service than a complex service.

Phase III: Security Testing & Evaluation. This phase (ST&E) is conducted to validate the security controls and verify that they have been implemented as documented in the planning phase. The aim of this phase is to ensure that all the security controls are implemented, and that they function properly, as expected, and in accordance with the policies, objectives, and standards laid out in Abu Dhabi Government documents. Also, this phase is conducted when new controls are added or changed during the system's life cycle, to ensure that they are performed effectively. The ST&E phase could be conducted by either an internal test team or an external party based on

the resource requirements and whether or not the system requires independent verification and validation.

There are several benefits to conducting the ST&E phase:

- Verification of the implementation of security controls.
- Assessment of the overall security posture of the information system.
- Promotion of a consistent approach to testing an information system.

Phase IV: Certification and Accreditation. Certification is a given when the security controls have successfully reduced the security risks to an acceptable level. The certification form shows that all the security controls of the services have been officially reviewed and are guaranteed to be working effectively. Accreditation means that a formal management decision has been made that a senior entity is allowed to make an operation in the information service. It is designed to inform senior government officials about the security risks and authorize the service to function. Since risk management is a mandatory process for all the systems in Abu Dhabi Government entities, the certification and accreditation phase is a requirement for all government services and will make those services more secure. If a government service has not been certified and accredited, all their functions should be stopped. This is another of the system owner's responsibilities, as he is responsible for securing the government service by developing, maintaining, procuring, and operating the information system.

The risk management process is applied to Abu Dhabi Government services whenever a major change is made that may affect the security of information. In any case, it is applied once every three years, to ensure that the information security system is updated to protect against current vulnerabilities and threats.

Injazat Data Systems Case Study

Injazat's (http://www.injazat.com) goal is to become the premier Information Technology (IT) and Business Process Services Outsourcing and Managed Services partner in the Middle East. It offers a broad range of services from IT strategy, IT consultancy, and systems integration to comprehensive outsourcing of IT and business functions. Injazat has the knowledge and the experience to manage, develop, and support the IT and business processes of government and private sector organizations.

This case study outlines Injazat's integrated ISO 27001 and ISO 20000 implementation approach, along with their underlying business rationale. It shows the value of applying best practices in line with ISO 27001 and ISO 20000 standards to encourage other organizations to implement and improve their own business environment.

We have interviewed the Injazat stakeholders involved in the strategic program to gain a fuller understanding of how they have implemented ISO standards in their organization: Adam Ali, the Senior Leader and a Board Member of the Middle East IT Service Management Forum promoting ITIL Service Management best practice and ISO 20000 certification; and Kamran Ahsan, the Information Security Officer of Injazat Data Systems.

Mr. Ahsan explained that Injazat's primary motivations for developing the ISMS program were:

- to further improve their information security posture and align it with an international standard;
- to establish a common understanding that would facilitate more effective communication on information security among the organization's various business units;
- to improve business practices; and
- to protect information assets.

In addition, Injazat wanted to gain higher levels of trust from its clients and partners by providing the best services in line with the company's aim of becoming the premier IT services partner in the Middle East.

The company followed the Plan-Do-Check-Act (PDCA) model for deployment of the ISMS. In the Plan phase, it identified the scope of the ISMS, wrote policies and procedures set up the security organization, and developed the ISRM framework. In the Do phase, Injazat focused on implementation and operations, and deployed ISRM in the data center environment. In the Act phase, the company began corrective and preventive actions to improve its ISMS program. Finally, in the Check phase, Injazat ensured compliance and the effectiveness of controls through an internal audit and results review.

Information Security Risk Management framework (ISRM). Injazat developed and adopted the Information Security Risk Management (ISRM) framework in its data center as a part of the ISO 27001 certification process. The framework is used in managing and assessing the IT and non IT infrastructure of the data center. In principle, it addresses six basic questions that can help organizations identify their strengths and weaknesses:

1. What can go wrong?
2. How can it go wrong?
3. What is the potential harm to our information assets?
4. What can be done to address potential harm?
5. How can we stop it from happening again?
6. How can we manage the entire risk environment of the business landscape?

Information Security Controls. Injazat has implemented a variety of administrative, technical, and physical security controls to more effectively protect itself. Administrative security controls are basically policies and procedures that define and guide employee actions in dealing with critical information, and ensure that these align with technical and/or physical security controls.

For example, the administrative policy could state that computers without antivirus software cannot be connected to the network. At the same time, technical controls, such as network access control software, will search for antivirus software when the computer tries to connect to the network. Physical security controls are devices that control physical access to sensitive places or information.

Physical controls go hand in hand with administrative policies to achieve the required objectives.

ISO 20000 Certification Process. The motivation for the program was to conform to recognized global standards for ITIL Service Management in line with Injazat's goal of emerging as the premier IT services provider in the Middle East.

Although the Injazat ITIL Service Management practice was to deliver IT Services within the framework, the company felt that achieving certification would support and strengthen the processes further and enhance the delivery function.

The ISO 20000 certification process commenced with a gap analysis aimed at identifying areas requiring conformance and enhancement, and evaluating the actual resources and activities required to complete the undertaking. Adam Ali was tasked with leading the ISO certification program with the support of the following departments:

IT Operations, ITIL Management, Applications, Ti2 Training, Procurement, Finance, Internal Auditing, Human Resource and Delivery Management, Systems and Service Management Tools, and the Internal Audit Team.

Injazat addressed the elements of ISO standards to ensure that they met the organization's IT requirements. These included Scope; Planning and Implementing Service Management; and Requirements for a Service Management System.

"There are synergies between ISO 20000 and ISO 27001 that made an integrated approach leveraging both standards highly appealing to us. For one thing, these standards highly prioritize security management by requiring in-depth Risk Assessment, impact analysis, and mitigation planning. They also mandate a high level of process control and managed service delivery. They support faster and more effective business decisions which are precisely integral to Injazat's core goals," says Adam Ali.

Guidelines for Integrating ISO 20000 with ISO 27001:

1. Planning phase. Injazat spent around five weeks on this phase, the most important part of the ISO certification process, which organizes the work in a structured manner. A security and risk management framework was set up at this time, while objectives such as identifying scope, writing policies, establishing a service management and security organization, and developing an Information Security Risk Management (ISRM) and ITIL Service Management Framework were also pursued.

2. Gap analysis. Before engaging in the certification process, Injazat had been addressing security problems based on its own internal protocols and adhering to the ITIL Service Management framework. After achieving certification, the company evaluated its current security and service management adherence against ISO best practices, which helped in identifying necessary improvements and in determining the appropriate steps and resources required for delivering enhancements. Injazat spent a significant amount of time updating policies, as well as process documentation and procedures, to them align with the standards and improve services even further.

3. Forums. Injazat established a regular service management and information security management system forum to follow up the ISO certification process, discuss and agree on strategies, oversee any risks or issues posed by the updated processes, and find the right solutions.

4. Training and awareness. Injazat developed customized training to deal with the diverse backgrounds and various comprehension levels of its employees, as these individuals have to be fully aware, first and foremost, of the security and service management program's importance to the organization. Injazat conducted various awareness sessions befitting the different objectives, tasks, and responsibilities of its various work groups. For example, the session for the service desk group was different from the sessions prepared for the network and security groups. Emails were sent out and security posters about passwords, ID cards, internet browsing, and malicious email attachments were strategically placed in the office areas to generate interest and develop awareness about information security.

A survey was also conducted to benchmark the current perception of IT Services, so that a recognized and agreed upon baseline could be determined.

Prior to the implementation of the ISO program, Injazat had invested in carrying out extensive ITIL Service Management training, leading to the certification of numerous operational and delivery management staff across the organization.

5. Internal Audit program. Injazat created an Internal Audit department, which ensures that employee and corporate activities comply with ISO standards.

The challenge after certification is to ensure that the objectives and benefits are not diluted and that Injazat can continue to provide value to its clients in a consistent manner, aligned with the business requirements of the organization and driving continuous service improvements.

Abu Dhabi Gas Industries Ltd. (GASCO) Case Study

We interviewed two individuals at Abu Dhabi Gas Industries Ltd. (GASCO) (http://www.gasco.ae/web/home/index.aspx) to gain a fuller understanding of the implementation of security standards in the UAE. The first was Asmaa Al Kindi, the company's project manager, who explained the process by which their IT department became ISO 27001 certified, which included benchmark assessment and external and internal audits. Based on the results of the benchmark assessment, they followed the PDCA cycle, in order to become certified (Abu Talib et al., 2011).

Ms. Al Kindi also explained that they had a detailed ISO 27001 certification roadmap, consisting of three phases: Gap analysis; implementation; and audit execution. The PLAN action involved defining the scope and the policy, establishing the security organization, and adopting a risk assessment framework (Stage 1). The DO action was concerned with the risk assessment (Stage 2), the internal audit program, and training and awareness. Finally, the CHECK and ACT actions involved monitoring the controls (Abu Talib et al., 2011).

In connection with this roadmap, GASCO had to complete the following steps in order to obtain the ISO certification: 1) Select an external accreditation body; 2) Submit an application; 3) Undergo the Stage I audit (review of ISMS documentation); 4) Fix the non conformities identified, if any; and 5) Undergo the Stage II audit (on-site assessment) (Abu Talib et al., 2011).

According to Ms. Al Kindi, employee awareness, security compliance, and management support were the success factors in the GASCO certification experience. Employee behavior and the employees' ability to accept change were two challenges that were faced during the certification process (Abu Talib et al., 2011).

Ms. Mona Younes, the company's Information Security Administrator, was the second person whom we interviewed. Ms. Younes built on what Ms. Al Kindi had said previously, explaining more about the ISO 27001 certification process and how they decided to follow the ISO 27001 framework based on their needs.

According to Ms. Younes, GASCO started the certification process in October 2007, and they became certified eight months later, in May 2008. The motivation behind developing the ISMS at GASCO was to help the organization improve their business practices and protect their information assets. Other goals were to improve the security controls of all their information systems and to enhance the confidence and awareness of their clients, stakeholders, and partners.

At GASCO, 70% of the IT crew were involved in implementing the ISMS program, with the contribution of other departments like HR and General Services. They used Deloitte, which offers its clients a broad range of auditing, tax, consulting, and financial advisory services on an outsourcing basis. GASCO chose Deloitte to take the first step in implementing the ISMS, which involves gap analysis and risk assessment.

Ms. Younes briefly explained the steps involved in following the ISO 27001 Roadmap to obtain certification. This process document outlines the steps to be taken by those who wish to obtain full ISO 27001 certification. The three main phases are: gap analysis, implementation, and audit execution. Each of these phases involves several steps, which must be achieved to complete the certification process.

Guidelines for ISO 27001 Certification Process

Phase I: PLAN Phase/Gap Analysis. The first step in the PLAN phase is to perform a gap analysis. GASCO used Deloitte Company to perform their gap analysis, which involved working through the cycle of assessing GASCO current security practices against best practices inspired by ISO 27001, identifying the gaps in the existing security controls, and defining the steps required to fill them. By completing this step, GASCO not only complies with the ISO 27001 standard, but also enhances their information security system performance.

In the PLAN phase, GASCO had a few objectives, which included identifying the information assets, system risks, policies and procedures used, and the updated policies and procedures. They defined the new policies from a review of the previous versions and updating them based on the recommendations of ISO 27001 standards.

Deloitte was responsible for writing the main ISMS documents for GASCO, such as ISMS policies and the disaster recovery plan. GASCO has 12 IT sections. The IT security team and three of those sections continued writing the ISMS documents, which involved one or two people from each section. Every IT section had its own policies and procedures that suited its needs and requirements. Examples of procedures included:

- Backup
- Employee Access Control
- Equipment Loan
- Information Security Incident Management
- Change Control
- Risk Management
- Information classification & Handling
- Document Change Control

Define ISMS Scope and Policies. The second step in the PLAN phase is to define the ISMS scope and policies, scope referring to its limitations and boundaries. In doing so, GASCO took the following steps:

- Define the scope of the ISMS (IT security function)
- Prepare an ISMS document
- Update the ABC’s of Corporate Information Security Policy
- Prepare an ISMS policy document in line with the ABC’s of Corporate Information Security Policy.

Security Section. GASCO established a security section in May of 2005 to handle the job responsibilities involved, which was supported by the managers. This section started with one person, but now there are seven employees working in it.

The company established this section by identifying the relevant stakeholders, and going on to define the security related responsibilities/roles and documenting them. Then, they established a Security Forum with the ABC's IT Steering Committee conducting meetings involving the discussion of actions to be taken based on the ISO standards, and the updated actions and their documentation. In addition, they developed the Security Forum charter, set the ISMS review periods, and drew up a meeting schedule. Finally, they approved and published the ABC’s of Corporate Information Security Policy.

Risk Assessment. The risks that GASCO faced included:

- Computer risks
- People risks
- Physical security
- Access control
- Password complexity risk

There are two ways to evaluate the risks: the qualitative method and the quantitative method. GASCO used the qualitative method, which involves conducting interviews and evaluating assets.

The company relied on Deloitte to carry out the risk assessment, which considers the core competence of ISMS implementation and maintenance. Deloitte started this phase by developing the risk assessment approach. They identified the information assets, threats, risks, and vulnerabilities that could have an impact on the confidentiality, availability, or integrity of any asset. After analyzing the risks, they evaluated and identified treatment options for them. Then, they selected control objectives and the associated security controls to be implemented. They obtained management approval for the residual risk related to implementing the ISMS program. Finally, they prepared a Statement of Applicability.

Phase II: DO Phase/Implementation

Risk Treatment. After the risk assessment phase was completed by Deloitte, the GASCO security team developed the risk treatment plan, which identified the appropriate management actions, resources, responsibilities, and priorities for managing information security risks. Based on the information we have, the security team focused on several areas in the risk treatment plan. They developed documents to support information security controls from ISO 27001, including:

- Human Resource Security
- Physical & Environmental Security
- Communications & Operations Management
- Access Control
- IS Acquisition, Development & Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

During the risk treatment process, the IT security team defined and deployed a measurement criterion, and planned for a security training & awareness project based on ISO 27001 requirements. They also developed SLAs/OLAs for the IT Security Team and IT Division interfaces. The SLA (Service Level Agreement) is an external contract between the IT Division and the other division(s) or department(s). The OLA (Operational Level Agreement) is an agreement that is internal to a division or department. Actually, GASCO had developed only SLAs for the IT Security Team and IT Division. In the final step of the risk treatment process, the IT Security Team developed ISMS-related documentation.

Internal Audit. Ms. Younes explained the internal audit for the ISMS program as follows: There were two sources for the audit: an internal group at GASCO that was responsible for auditing the whole organization annually; and a third-party auditor, which was Deloitte. As the internal audi-

tor, Deloitte reviewed all the ISMS documentation, policies, and procedures, observed employee behavior, and gave their feedback to GASCO. Furthermore, they performed penetration testing to check whether or not the system had any weaknesses or vulnerabilities. In the beginning, Deloitte conducted the internal audit every six months, but now they conduct it every eight months.

Training and Awareness. According to Ms. Younes, GASCO had a complete security training and awareness program in place for all its employees. Several methods were used to train them and raise their awareness about the new ISMS. Examples of these methods include giving presentations presenting the ISMS and the changes and improvements that it would bring to the organization. They also prepared posters and regularly sent awareness emails to all employees. In addition, they held numerous information sessions at all the remote sites and other branches associated with GASCO. However, they did not provide any technical training for the employees. There were also quizzes for the employees after the sessions to measure their understanding of the system and to continue the awareness process. Ms. Younes added that accepting the changes to the whole security system was somewhat difficult for the employees, since it changed the way specific tasks were performed, and might result in them being more time-consuming. For example, before the ISMS was implemented, the employees could go to the IT department and simply ask them to perform a particular task, but, after implementing the security system, the employees had to go through several steps (open a ticket, log events, etc.) to authorize the IT department to help them. This new awareness enhanced the information system and made it possible to keep things on track. Ms. Younes added that the most challenging obstacle they faced was employee behavior, as the employees found it difficult to make changes, adapt to new situations, and change old habits. In the beginning, when GASCO started applying the ISMS program, the changes were not accepted quickly; however, after a while they adapted to the changes and saw their benefits. With employee awareness about the importance of security compliance and the support of management, GASCO obtained the certification.

Phase III: CHECK and ACT Actions/Audit Execution

Monitoring Controls. GASCO monitored the ISMS and implemented the controls. They also started to perform the internal ISMS audit. However, they still needed an ISMS expert to carry out the audit for them, so they used DELOITTE, the firm that had been performing the risk management testing for GASCO every six months, and now every eight months. In addition, GASCO conducted a management review of the results, and remedied the non conformities that were identified.

Certification Process. As a first step in the Certification process, GASCO selected an external accreditation body, Lloyd's Register, to conduct the assessment, which consisted of two stages (a Stage 1 audit, and a Stage 2 audit), in addition to an intermediate process between the two. In the Stage 1 audit, Lloyd's reviewed and checked all the ISMS documentation. GASCO remedied the non conformities that the external audit had identified. The Stage 2 audit consisted of an on-site assessment, and included interviewing employees and ensuring staff awareness. Now that certification has been obtained, the external auditing firm conducts annual checkups, and performs a reassessment every 3 years.

Table 4 analyzes the three case studies and puts some remarkable conclusions.

Table 4 Study cases analysis and conclusions

	ADSIC	Injazat Data Systems	GASCO
Guidelines	Guidelines for following ISO 270001 standard and expands on it using additional management processes based on the organization needs	Guidelines for integrating ISO 20000 with ISO 27001	Guidelines for ISO 27001 certification process
Plan Do Check Act (PDCA) Model	The Risk Management Process is an ongoing one, which is guided by PDAC model to determine which controls are required, and basically to allow the implementation of the right security controls in order to address all risks.	PDCA is followed for deployment of the ISMS in Injazat Data Center for managing and assessing the IT and non IT infrastructure.	Based on the results of the benchmark assessment, they followed the PDCA cycle, in order to become certified.
Planning Phase	Risk Assessment phase promotes a consistent approach to measuring risks and allows stakeholders to place values on potential losses.	It identifies scope and policies, establishes a service management and security organization, and develops an Information Security Risk Management (ISRM) and ITIL Service Management Framework is also pursued.	It is about identifying the information assets, system risks, policies and procedures used, and the updated policies and procedures. It also includes ISMS scope and policies.
Gap Analysis	Information Security Planning phase helps in selecting the controls that address the security risks, and in documenting the planned and implemented controls for the information system. Security issues must be addressed continually, which makes planning for information security an ongoing process.	Addressing security problems based on Injazat internal protocols and adhering to the ITIL Service Management framework.	Using Deloitte Company to perform their gap analysis, which involved working through the cycle of assessing GASCO current security practices against best practices inspired by ISO 27001
Internal Audit	Security Testing & Evaluation is conducted to validate the security controls and verify that they have been implemented as documented in the planning phase. It could be conducted by either an internal test team or an external party based on the resource requirements and whether or not the system requires independent verification and validation.	Injazat created an Internal Audit department, which ensures that employee and corporate activities comply with ISO standards.	There were two sources for the audit: an internal group at GASCO that was responsible for auditing the whole organization annually; and a third-party auditor, which was Deloitte. Furthermore, they performed penetration testing to check whether or not the system had any weaknesses or vulnerabilities. In the beginning, Deloitte conducted the internal audit every six months, but now they conduct it every eight months.
Challenges	- If a government service has not been certified and accredited, all their functions should be stopped. - The risk management process is applied whenever a major change is made that may affect the security of information. In any case, it is applied once every three years.	The challenge after certification is to ensure that the objectives and benefits are not diluted and that Injazat can continue to provide value to its clients in a consistent manner, aligned with the business requirements of the organization and driving continuous service improvements.	Employee behavior and the employees' ability to accept change were two challenges that were faced during the certification process.

Conclusions and Future Work

Information security is considered as a concern for all organizations. “The total number of security incidents reported to the CERT (Computer Emergency Response Team) rose from 2,412 in 1995 to 82,094 in 2002” (Purser, 2004). The use of IT standards could be one way to protect sensitive information within an organization. This survey study explains the wide applicability of IT standards in various sectors in the UAE, the advantages and disadvantages of using these standards, and organizations’ future need for IT standards. Three cases studies in three contexts are detailed. The first is on the Abu Dhabi Systems and Information Centre (ADSIC). Their program is consistent with the ISO 27001 framework, and they have expanded it using additional management processes. The second is on Injazat Data Systems. They used the integrated ISO 20000 - ISO 27001 approach to mandate a high level of process control and managed service delivery. The integrated approach supports faster and more effective business decisions, which are integral to Injazat’s core goal. The third case study is on the security certification process at Abu Dhabi Gas Industries Ltd. (GASCO). To summarize our findings, these three case studies can be used as a practical guide to implement ISO 27001 within an organization. As this research indicates the importance of applying standards within an organization therefore, producing graduates with that knowledge in Information Security domain is required. Integrating ISO standards to IT curriculums could be a future work for this study. We can also consider comparative studies globally in terms of costs, company types, limitations, procedures and processes and advantages and disadvantages.

Acknowledgment

We thank Ms. Asmaa Al Kindi and Ms. Mona Younis of GASCO, Mr. Mohamed Karmastaji of ADSIC, Mr. Adam Ali and Mr. Kamran Ahsan who contributed to our study in this research. Thanks, too, to Zayed University students who helped in collecting data.

References

Abu Talib, M., Khelifi, A., & El Barachi, M. (2011). Exploratory Study on Innovative Use of ISO Standards for IT Security in the UAE, submitted to European, Mediterranean & Middle Eastern Conference on Information Systems 2011 (EMCIS2011), May 30-31 2011, Athens, Greece.

The Australian Council on Healthcare Standards [ACHSI] (2011). URL: http://www.achs.org.au/

Emirates Authority for Standardization & Metrology [ESMA]. (2010). Abu Dhabi. Retrieved from http://www.esma.ae/lang-en

Fenton, N., & Bieman, J. (in press). *Software metrics: A rigorous and practical approach*, Chapter 4. (3rd ed.). CRC Press.

Hommes, L., & Hommes B. (2004). *The evaluation of business process modeling techniques*. Doctoral thesis (2004). Technische Universiteit Delft.

The Information Systems Audit and Control Association (ISACA). (2011). URL: https://www.isaca.org/

International Atomic Energy Agency, Austria. (2011). URL: http://www.iaea.org/

Information Technology Infrastructure Library. (2007). Retrieved from http://itsm.fwtk.org/index.htm

International Organization for Standardization [ISO]. (2010). Switzerland URL: http://www.iso.org/iso/home.html

ISO/IEC 27001. (2005). *Information security management systems – Requirements*. International Organization for Standardization – ISO, Geneva

ISO/IEC 27002. (2005). *Code of practice for information security management.* International Organization for Standardiza-tion – ISO, Geneva.

ISO/IEC 27006. (2005): *Requirements for bodies providing audit and certification of information security management systems*. International Organization for Standardization – ISO, Geneva.

Microsoft Solutions Framework Certification. (2011). URL: http://www.ehow.com/facts_7490389_microsoft-solutions-framework-certification.html

Purser, S. (2004). *A practical guide to managing information security*. Norwood, MA: Artech House.

Richards, S., & Dar, R. (2009). Standardization & classification in the UAE. Al Tamimi & Company. Retrieved from http://www.thyh.com/Publications/International/Standardization%20and%20Classification%20in%20the%20UAE.pdf

Software Engineering Institute, Pittsburgh, USA. (2010). URL: http://www.sei.cmu.edu/cmmi/

Telecommunications Industry Association, Arlington. (2011). Retrieved from http://www.tiaonline.org/standards

Timmons, K. (2003). Delivering quality care through accreditation: The why, what and how of JCI accreditation. *Hospital Management Asia 2003*, Philippines.

Biography

Manar Abu Talib is an Assistant Professor in the College of Information Technology at Zayed University, Abu Dhabi. She received her PhD in Computer Science and Software Engineering from Concordia University, Montreal, Canada, in 2007. Dr. Abu Talib's research interest include software engineering with substantial experience and knowledge in conducting research in software measurement, software quality and in real-time systems analysis, design, and testing. Her Teaching interests are Programming, Web Development, Information Security, Software Engineering, Software Measurement, Software Quality and Software Testing and Entrepreneurship. She is working on ISO standards for measuring the functional size of software, and has been involved in developing the Arabic version of ISO 19761 (COSMIC-FFP measurement method) at Zayed University. She has an impressive list of papers to her credit, which have most recently been accepted by journals in Canada, Italy, and Germany.

May El Barachi holds a Ph.D. and a Masters degree in Electrical and Computer Engineering from Concordia University (Canada) and a Bachelor degree in Electronics and Telecommunications Engineering from the Arab Academy for Science and Technology (Egypt). She carried her masters and doctoral research as part of an industry/academia cooperation program established between R&D Ericsson Canada and Concordia University, and participated in several projects related to key areas in the networking field within that program. She was also part of the IST Ambient Networks project - a European Union (EU) 6th framework project, and worked as a Postdoctoral fellow at the University of Quebec – School of Superior technology (ETS). Presently, she is an assistant professor at Zayed University (UAE). Her current research interests include: service engineering; quality of service and adaptive resource management, context-awareness, web services, virtual networks, wireless sensor networks, and next generation networks. In these areas, she has authored many peer-reviewed papers and has one accepted patent.

Dr. Adel Khelifi is Associate Professor and Chair of the Software Engineering department at ALHOSN University, UAE. With a PhD from the Engineering School of High Technology, Canada (2005), a Master from the University of Quebec, Canada (2001), Diploma from the National Centre of Computer Science, Tunisia (1995) and a Bachelor degree in Industrial Engineering from Annaba University, Algeria (1991), Dr Khelifi holds a high level of knowledge and expertise. Currently Dr Khelifi is involved in developing Software Engineering courses' content including software quality, software testing and software maintenance for the students.

Dr Khelifi has held impressive past careers, most recently working as a lecturer for the Engineering School of Technology in Canada and previously working for United Nations MSF in Canada, Ministry of Relations with Citizen and Immigration in Canada and Ministry of Finances in Tunisia. As a Canadian ISO member in Software Engineering, Dr Khelifi is contributing in developing Open Source Software.

Dr. Olga Ormandjieva is Associate Professor in the Computer Science and Software Engineering department at Concordia University, Montreal, Quebec (Canada). She is also a member of the Ordre des Ingénieurs du Québec (OIQ). She has a Ph.D. in Science Degree (2002) and Master's Degree in Computer Science and Mathematics (1987). The main area of research of Dr. Ormandjieva is Measurement in Software Engineering and its extension to the development of formal methods for modeling and monitoring of reactive autonomic systems? functional and non-functional features with category theory. Her strategy for research and publications has been to create strong foundations for independent research, publish in top workshops and conferences supported by IEEE and ACM, and then target international good quality journals in the field. Currently Dr. Ormandjieva is teaching software engineering undergraduate and graduate courses at Concordia University.