

# ISO 27001 Gap Analysis - Case Study

Ibrahim Al-Mayahi, Sa'ad P. Mansoor

School of Computer Science, Bangor University, Bangor, Gwynedd, UK

**Abstract**—This work describes the initial steps taken toward the development of an Information Security Management System for the UAE e-government. To achieve this goal it was decided to obtain the ISO 27001 certification, which is the leading standard in information security. Gap analysis was performed on four selected organisations within the UAE e-government to determine their compliance against the ISO 27001 standards. This process will help identify the weakness in the existing system and highlight the any associated risks to the UAE e-government. In this paper a Management, Technical and Operational (MTO) model is presented. This model gives greater focus and provides a framework which is more aligned to the organisations structure and responsibilities. The results of benchmarking based on the ISO27001 standard, and the method used to measure the maturity level for each security control domain are presented.

**Keywords:** Gap Analysis, ISO27001, Compliance, Information Security, Auditing

## 1. Introduction

Information security is critical for todays organisations, global exposure to threats means that they must protect themselves from external and internal threats. Wiander [1] describes the importance of building an information security management system based on ISO 17799 standards. The study concludes that there was internal resistance to change and this was due to lack of information available to the employees within the organisation. Valdevit et al. [2] shows that there is growing interest from SMEs to be ISO27001certified in order to improve their IT security and to achieve that; a suitable GAP analysis tool was developed.

In his paper Dey [3] describes the development of an information security system, and show that there should be proper analysis and design, involving the entire organisation, starting from the senior management to the end users. The conclusion was they all should take appropriate roles in establishing and implementing of an information security system within the organisation. Technology solutions need to be implemented appropriately to fight against threats and risks or to automate certain processes. Policies and procedures need to be established in order to define who will do what, when and how, in order to prevent the threats. A detection mechanism is required and once a thread is detected, it will take corrective measures to fix any damages.

There should be a cultural change too within the organisation to deal with information and its security in general.

The concept of an e-government is to provide access to government services to the public sector (citizens and businesses) at anytime over an open network. This leads to issues of security and privacy in the management of the the information systems. To develop a secure e-government system the organisations involved, is required to have an ISMS (Information Security Management System). The reason to develop the ISMS for the UAE e-government was strategic decision agreed by the management board, to meet the following organisational requirements [4]:

- A central government requirement to develop the UAE e-government.
- The desire to meet various regularity requirements, particularly around computer misuse, data protection and personal privacy.
- To manage information more effectively for each organisation within the e-government.

To measure the risks of data misuse, loss, or disclosure organisations normally implement a number of security controls. In the UAE e-government case it was decided to use a suitable security standard as a benchmark. The objectives of the standard itself is to provide a model for establishing, implementing, operating, monitoring, reviewing and maintaining the information system, based on a business risk approach. Most organisations, in order to ensure compliance with the various regulations and corporate governance rules around securing key information, adopt the ISO27001 standard. The compliance assessments evaluate 133 controls of the requirements that are designed to achieve the 39 objectives of the standards within 11 key domains [5].

The objective of this research is to prepare the groundwork for the development of the UAE e-government, and to achieve that it is important to implement Information Security Management System. Four different organisations within the UAE e-government were used as case studies. All these organisations manage and operate their own information security, which implies that they are running an implicit Information Security Management System without a systematic risk assessment according to ISO27001.

There are some of main known risks that have been identified, but the problem is they are not properly classified and no methodology is implemented to deal with these risks. Furthermore, there is no document procedure to control the whole setup, which implies that there is no clear overview

that exists about whether actions are taken or not. Thus, a risk management system must be implemented and the gap analysis is the first step toward achieving this.

## 2. GAP Analysis

Compliance is the process of comparing the applied controls of an organisation with those in ISO27001 in this case. The Gap analysis is a tool or a technique that enables an organisation to compare its actual performance with the standards [6]. It is different from risk assessment in the fact that it compares the object against some target (that could be desired performance level or standard), whereas risk assessment is not measured against a target. Both Gap analysis and risk assessment evaluate the answer to "*where are we?*" but in the case of Gap analysis it is measured against "*where we want to be*".

For this study the four different organisations that were used as case study's were the core electronic service departments under UAE e-government. The gap assessment was initially carried out on the information that has been shared with section managers on a sample basis. Sample cases were taken in each of the areas to check the compliance to the standard. The next step was to assess the compliance of all the sections within the chosen departments. This was achieved by interviewing the relevant managers and their teams to have a clear picture of the business, reproducible results and consistency, together with the review of documentary evidence in order to verify the compliance level. Table 1 shows a list of the 11 key domains and the people responsible for each of them.

Table 1: List of interviewees for each Domain

Domain	Interviewee
A5 Security Policy	Director & All Teams
A6 Organisation of Information Security	Head of Electronic Audit
A7 Asset Management	Head of Quality Management
A8 Human Resources Security	Head of Network & Operations
A9 Physical and Environmental Security	Head of Cyber Crimes Section
A10 Communications & Operation Management	Local Branch
A11 Access Control	Data Entry
A12 IS Acquisition, Development & Management	Consultant
A13 Information Security Incident Management	Database Specialist
A14 Business Continuity Management	Management Team
A15 Compliance	Legal Departement

## 3. MTO Model

The ISO27001 eleven security domains do not provide insight into which group in the organisation is responsible for an activity. Thus, as part of this research a model based on the organisations structure was developed. This model provides greater focus and better understanding on where within the organisation the responsibility lies for each domain. The security domains are grouped into three categories based on responsibility:

- Management Controls, which include the following domains: security policy, organisation of information security and compliance.
- Technical Controls, which include the following domains: asset management, physical and environmental security and communications & operations management.
- Operational Controls, which include the following domains: systems acquisition, development & maintenance, access control, IS incident management and business continuity management.

This model provides a common language for all to view and manage information security activities. It could be considered as a framework for measuring and monitoring performance and integrating better management practices, which are more aligned to traditional organisational structure and responsibilities.

## 4. Maturity Model

The concept of maturity models is used regularly in the field of Information Systems as an approach for organisational assessment. Any systematic framework for carrying out benchmarking and performance enhancement that has continuous improvement processes, can be considered a maturity model. Generally, in the constituent literature, maturity implies perfect or explicitly defined, managed, measured, and controlled systems [7]. It is also a progression in the demonstration of a specific ability or in the accomplishment of a target from an initial to a desired end stage.

There are common mature modules available and these are NIST, CITI-ISEM, COBOT, SSE/CM and CERT/CSO and all these have between 5-6 levels of maturity, and for the purpose of this study it was decided to use the COBIT model, because it is focused toward auditing specific procedural awareness and adaptation [8],[9]. The COBIT Maturity Model is an IT governance tool was used to measure how well the management processes are developed with respect to internal controls. Such capability can be exploited by auditors to help management fulfil its IT governance responsibilities.

A fundamental feature of the model is that it allows the organisation to measure its current maturity level against a specific standard, in this case ISO27001. As a result, it can discover practical improvements to the internal controls

of the IT system. The maturity levels are not a goal, but rather they are a means to evaluate the adequacy of the internal controls with respect to the e-government business objectives [10]. The model focuses on auditing specific procedures. This definition of maturity has several important characteristics:

- Provides the blueprint for a complete security program.
- Inform management of the order in which to implement security elements.
- Leads toward the use of best practice standards (in our case the ISO 20071).

This approach toward a detailed security maturity model (Security Program Maturity Model) takes a management systems approach. It involves the existence or non-existence of the 11 controls (domains) which comprise the ISO27001. A list of questions was used to capture the compliance of the organisation under different scenarios, and also to establish the maturity level for each of the 11 controls.

The maturity values are determined by the security requirements of the organization. During implementation two issues needed to be addressed the questions and their maturity values. This was resolved by designing the questions using the ISO27001 standard controls and carefully determining and agreeing on their maturity values (weight). Below is the list of agreed maturity values and their description:

- Nonexistence (0): there is no recognition of the need for internal control.
- Ad-hoc (1): there is some recognition of the need for internal control.
- Reputable but initiative (2): controls are in place but are not documented.
- Defined (3): controls are in place and are adequately documented.
- Managable and measurable (4): there is an effective internal control and risk management environment.
- Optimize (5): An organisation wide risk and control program provides continuous and effective control and risk mitigation.

To establish the initial maturity benchmark, the relevant staff were contacted from the four departments. Then, they were interviewed individually, and asked to answer the questions related to their domain.

## 5. Gap Analysis Results

The current levels of compliance against the principle of code of practices have been categorised using the following definitions:

- Compliant: The organisation is fully compliant with the specific are of ISO27001.
- Partially compliant: The organisation has gone some way towards being compliant, but still requires additional work to be undertaken.

- Non-compliant: The organisation does not have the controls in place to satisfy the requirement of ISO27001.

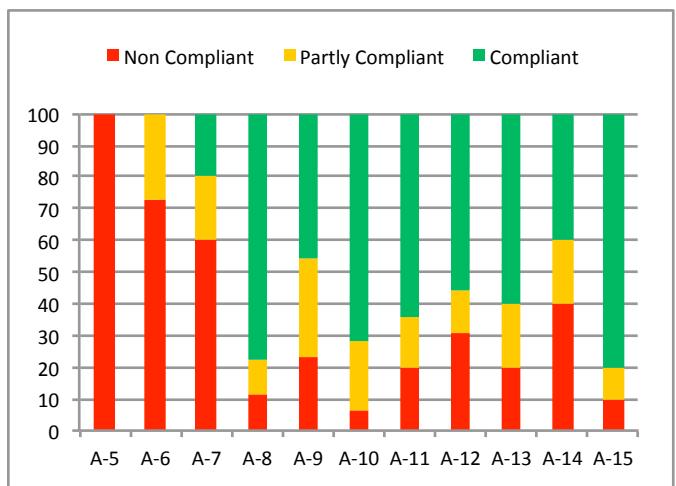


Fig. 1: Gap analysis compliance level

The result shown in Figure 1 indicates that some of the controls are more mature than others; it is evident that control A-5 show 100% non-compliance. This is due to the nonexistence of an approved security policy. It can be seen that the controls A-6 and A-7, exhibit high percentage of non-compliance, and once again this is due to the lack of implementation of effective security policy within these two controls. While the rest of the controls seems to have higher percentage of compliance and this is due to internal security procedure being put in place by the team responsible for each section.

The next analysis carried out was to identify the compliance of each section of the organisation based on the MTO model. The result is shown in Figure 2, and it is clear that the management has more than 60% non-compliance, this is primarily due to lack of information security policy. Meanwhile the technical and operation sections have higher percentage of compliance and this is due to internal security measures put in place.

Table 2 shows the compliance level for all the 133 requirement controls, and it can be seen that:

- 56.4% of the controls that were reviewed found out to be compliant with ISO27001 standards.
- 18.8% of the controls that were reviewed found out to be partly compliant with ISO27001 standards.
- 24.8% of the controls that were reviewed found out to be non-compliant with ISO27001 standards.

This indicates that there are large number of controls that meet the standard required, and bearing in mind that this is the first attempt to test the organisation compliance, it is quite an encouraging outcome.

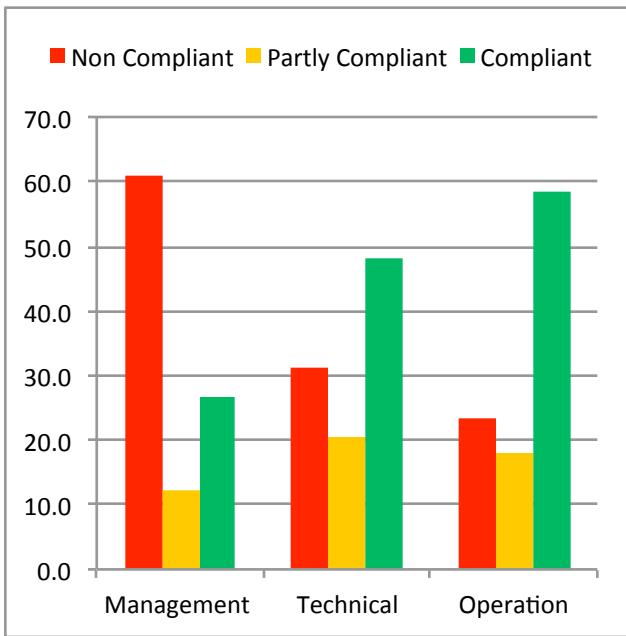


Fig. 2: MTO model results

Table 2: Domain compliant level

Domain	Req.	Compliant	Partly compliant	Non compliant
A-5	2	0	0	2
A-6	11	0	3	8
A-7	5	1	1	3
A-8	9	7	1	1
A-9	13	6	4	3
A-10	32	23	7	2
A-11	25	16	4	5
A-12	16	9	2	5
A-13	5	3	1	1
A-14	5	2	1	2
A-15	10	8	1	1
<b>Total</b>	<b>133</b>	<b>75</b>	<b>25</b>	<b>33</b>

Figure 3 displays the results of the maturity benchmarking against ISO27001, and the scores used for benchmarking are explained below:

- Maturity score below 1.65: The organization should start implementation of overall security measures.
- Maturity score between 1.66 and 3.25: The organization has taken significant steps to enhance security.
- Maturity score above 3.26: The organization fulfills defined measures, thus the probability of high risks is marginal.

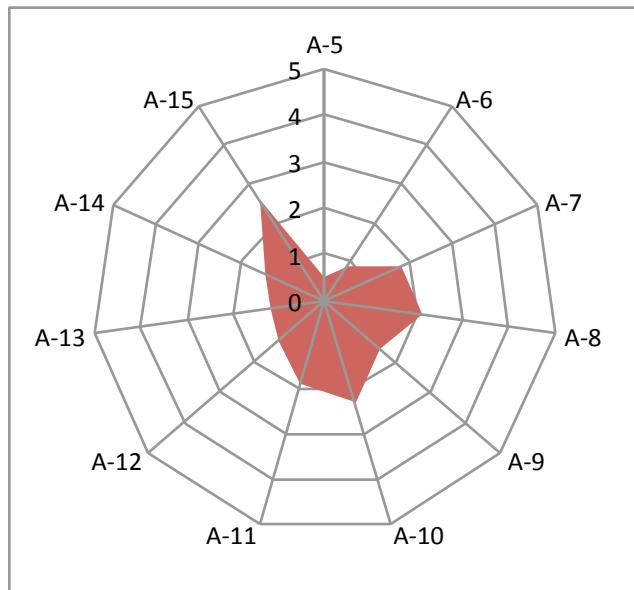


Fig. 3: Maturity benchmarking for each domain

It is obvious that some of the controls are more mature than others, for example the compliance, communication human resources security and asset management score lies between 1.67- 3.25. This implies that work has been done to improve the security of the organisations involved in this research. In the meantime there are some controls that lie in the reign below 1.65, which implies that the operation is dependent on knowledge and motivation of individuals, many control weaknesses exist and are not adequately addressed. Employees may not be aware of their responsibilities, and action is required to improve the security of these controls.

## 6. Conclusions

An information security management system is an integral part of an organisations management it is required to monitor, review and improve the information security of the organisation. It is a continuous process that deals with security policy development, and put procedures in place to deal with security threats. The gap analysis is initially used to identify the weaknesses in the organisations procedures. This should be a continuous process, as the organisation is required to be revisited to update the gap analysis. This is carried out to ensure long term protection against security breaches.

The security that can be achieved through technical means is limited, and should be supported by appropriate policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all stockholders including, employees, suppliers, third parties and other external parties.

## Acknowledgements

The authors would like to thank the UAE Ministry of Interior and the UAE Ministry of Higher Education for supporting this work.

## References

- [1] T.Wiander, "Implementing the iso/iec 17799 standards in practice: experience on audit phases," in *Proc. Australian Information Security Conference (AISC2008)*, 2008.
- [2] T.Valdevit, N.Mayer, and B.Barafot, "Tailoring iso/iec 27001 for smes: A guide to implement an information security management system in small settings," in *Proceeding of the 16th European Systems & Software Process Improvement and Innovation Conference*. Springer Berlin Hiedelberg, 2009.
- [3] M.Dey, "Information security management - a practical approach," in *Proceeding AFRICAN 2007 Conference*, 2007.
- [4] A.Calder, *Information Security Based on ISO 27001/ISO 17799: A Management Guid.*. Van Haren Publishing, 2006.
- [5] *Information security management systems requirements*, International Standards ISO/IEC 27001 Std., 2005.
- [6] B.Karabacak and I.Sogukainar, "A quantitative method for iso 17799 gap analysis," *Computers and Security Journal, Elsevier*, vol. 25(6), pp. 413–419, 2006.
- [7] A.Pederiva, "The cobit maturity model in a vendor evaluation case," *Information systems Control Journal*, vol. 3, 2003.
- [8] S.Woodhouse, "An isms (im)-maturity capability model," in *IEEE 8th International Conference on Computer and Information Technology Workshops*, 2008.
- [9] C.S.Leem, S. Kim, and H.J.Lee, "Assessment methodology on maturity level of isms," *Knowledge-Based Intelligent Information and Engineering Systems*, vol. Pt 3, Proceedings. vol. 3683 Springer-Verlag Berlin, pp. 609 – 615, 2005.
- [10] S. B.Tuttle, "An empirical examination of cobit as an internal control framework for information technology," *International Journal of Accounting Information Systems*, vol. 8, pp. 240 – 263, 2007.