A NEW FRAMEWORK FOR BRIDGING THE GAP BETWEEN IT SERVICE MANAGEMENT AND IT GOVERNANCE FROM A SECURITY PERSPECTIVE

E. da Cruz[1] and L. Labuschagne[2]

Academy of Information Technology
at the University of Johannesburg

PO Box 524

Auckland Park

Johannesburg

2006

1. eddycruz@softhome.net

(072) 480 4262

2. ll@rau.ac.za

(011) 489-2847

ABSTRACT

With COBIT and ITIL at the forefront of IT governance and IT service management, respectively, there is a need to establish if ITIL Security Management complies with COBIT DS5. This paper investigates the possible compliance and any related issues by comparing the requirements of COBIT DS5 against the measures of ITIL Security Management. Results indicate that ITIL Security Management is unable to fully comply with COBIT DS5. An attempt is made to offer a possible solution through the use of an additional framework that may be integrated into ITIL so that compliance with COBIT DS5 can be achieved.

KEYWORDS

ITIL, COBIT, IATF, security, cryptography, encryption, certificates, keys, IT governance, IT service management

A NEW FRAMEWORK FOR BRIDGING THE GAP BETWEEN IT GOVERNANCE AND IT SERVICE MANAGEMENT FROM A SECURITY PERSPECTIVE

1 INTRODUCTION

IT investments grew drastically during the technology “boom” days of the 1980s and early 1990s. Between preparations for Y2K and the dot-com boom, it appeared as though no cost was too great and no business case too spurious for technology investments (Williams, 2002). This caused massive spending on IT, with little or no formal method of managing and controlling IT resources.

Today, IT systems are constantly expected to improve return on investment, increase service levels and enhance security all without increasing costs, giving greater importance to IT governance (Spafford & Gene, 2004). Over the years a number of models and frameworks have been developed and put forth into organisations with the goal to improve the management of IT and IT related resources.

One framework, known as COBIT (Control Objectives for Information Technology) focuses on IT governance and it is directed at a number of target audiences from IT managers to auditors (IT Governance Institute, 2000). It is currently in its third revision and is developed by the IT Governance Institute. COBIT attempts to provide IT governance at the tactical level by means of a structured approach using controls and performance metrics.

In contrast, ITIL (the IT Infrastructure Library) focuses on the operational level of the organisation, providing “best practice” guidelines and architectures to ensure that IT processes are closely aligned with business processes (OGC, 2002). It is the most widely used and accepted approach to IT service management in the world (Rudd, 2004).

IT governance and IT service management have become the focus of IT with organisations implementing both COBIT and ITIL. Although both frameworks have the objective of improving IT efficiency and effectiveness, there is no formally documented mapping between these frameworks. Without a formal mapping between COBIT and ITIL, a manager using COBIT at the tactical level is unable to verify that the necessary measures have been implemented at the operational level using ITIL or a similar framework. In today’s litigious society, managers and executives need to be sure that they have performed their duties as they are held personally responsible for their actions or lack thereof. A mapping between ITIL and COBIT will provide the necessary structure and means to measure compliance of the tactical controls at the operational level.

This paper focuses on mapping ITIL Security Management against the security component of COBIT (formally known as COBIT DS5). Research for this paper was performed in a quantitative manner involving analysis of both frameworks at a detailed level and also includes qualitative research by means of interviews with organisations that use both COBIT and ITIL.

This paper’s layout consists of a mapping between the ITIL Security Management measures against the COBIT DS5 objectives requirements. Through this mapping, it will become clear if there are any links and shortfalls. Should there be shortfalls, an attempt will be made to offer a possible solution to better connect COBIT and ITIL from a security perspective.

2 MEASURES AND REQUIREMENTS

Before investigating a mapping between COBIT and ITIL, the organisational structure has to be considered, as COBIT and ITIL function at different levels. An organisation has three levels, namely strategic, tactical and operational. The operational level itself is on top of a "data" level. This data level consists of all the data that is generated through the daily business processes and needs to be processed so that it may be carried up through to the higher levels of the organisation as shown in figure 1.

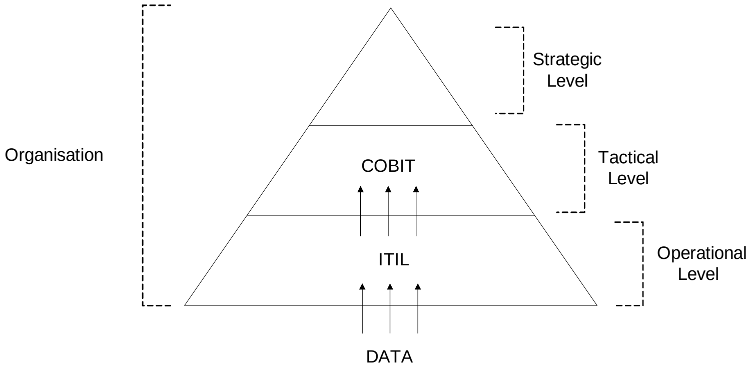
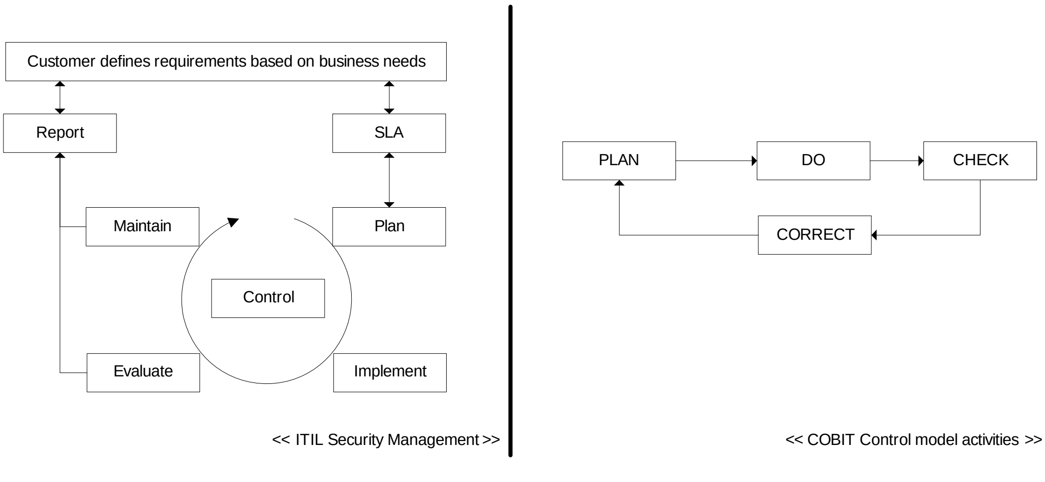


Figure 1. The various levels in an organisation with COBIT and ITIL

COBIT focuses on the higher level aspects of management and IT Governance placing it in the tactical level. Although ITIL does state that it can operate at all three organisational levels, the author believes that it functions at the operational level as ITIL is oriented to improving service delivery and support (John Morency, 2005).

To successfully map COBIT and ITIL security, it is necessary to extract what ITIL security provides and what COBIT security requires. In this context, a "measure" is some control or process to meet some end and can be measured. In a similar fashion, the "requirements" for the COBIT DS5 objectives will also have to be extracted. The requirements in this context are the necessary controls or measures that need to be implemented to satisfy the respective control objectives.

As this paper is about security, the focus is on the high level control objective from COBIT entitled Ensure Systems Security (DS5). This control objective addresses all aspects of security from policies and procedures to security functions. ITIL security is grouped in a component known as Security Management. The ITIL Security Management process and the COBIT control model activities are shown in figure 2.



Customer defines requirements based on business needs
Report
SLA
Maintain
Plan
Control
Evaluate
Implement
<< ITIL Security Management >>
PLAN
DO
CHECK
CORRECT
<< COBIT Control model activities >>

Figure 2. ITIL Security Management and COBIT control model activities (OGC, 2002; IT Governance Institute 2000)

The ITIL component consists of six main processes, some of which contain security measures, flowing in a clockwise direction and are iterative. The COBIT control model activities (formally known as IT Activities) used by management are very similar to Security Management as figure 2 illustrates.

The security requirements found in ITIL Security Management are clearly labelled and have a brief summary that describes their aspects. However, the part of the measure that is to be measured is not clearly stated. This “measurable” part was extracted by identifying the elements that existed within the security measure. A similar process was followed for the requirements of the COBIT objectives. It is these elements that are a requirement for a mapping.

3 SECURITY MAPPING MATRIX

The mapping of COBIT and ITIL is done using a matrix enabling the reader to visually see any correlations. The matrix will map the security measures of the ITIL Security Management processes against the COBIT DS5 objectives. Any objectives that are not matched are then explored in further detail. Figure 3 shows the overall scheme of the mapping matrix.

When considering the background of both frameworks, one is able to reasonably state that there should be a partial mapping as both COBIT and ITIL are based on ISO 17799 (IT Governance Institute 2000; OGC, 2002), which should provide some common ground. For reasons of briefness, the full mapping matrix is not included in this paper.

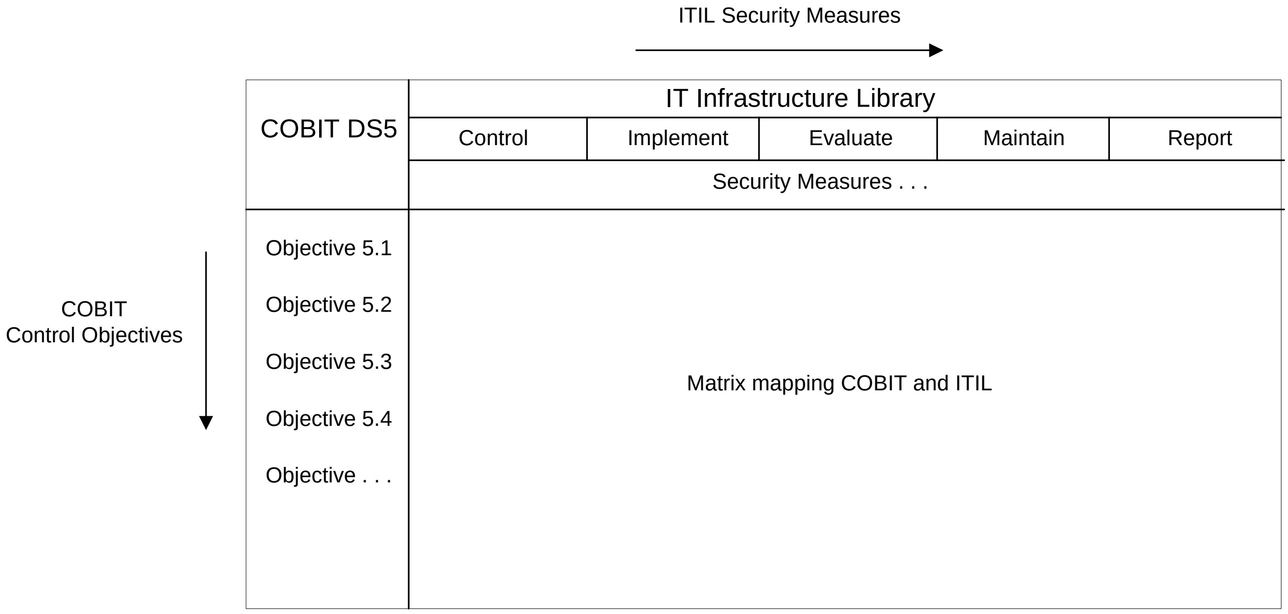


Figure 3. COBIT - ITIL security mapping matrix

The results of the mapping matrix indicate that most of the ITIL measures map onto some control objective. While there is a reasonably “good” mapping, there are five control objectives that are not addressed by the ITIL security measures. Even though a perfect fit does not exist, the assumption made of a partial fit was proven true and is supported by the COBIT-ITIL mapping done by the IT Governance Institute (IT Governance Institute, 2004). It should be noted that the mapping process mapped which ITIL measures address the respective control objectives, be it partly or completely. In some cases an ITIL measure addressed more than one COBIT objective and vice versa.

These five COBIT control objectives (hereafter referred to as the unmatched control objectives) are:

- Counterparty Trust (Detailed Objective 5.13)
- Transaction Authorisation (Detailed Objective 5.14)
- Non-repudiation (Detailed Objective 5.15)
- Trusted Path (Detailed Objective 5.16)
- Cryptographic Key Management (Detailed Objective 5.18)

When investigating these unmatched control objectives, a common theme can be identified amongst them, namely cryptography. This is of significant importance as ITIL Security Management does not explicitly address cryptography.

With the initial mapping of COBIT and ITIL security complete, a gap centred on cryptography is evident, preventing an organisation from using ITIL Security Management on its own to fully comply with COBIT DS5. This indicates that additional measures within ITIL Security Management or an additional framework are required.

Having identified this shortfall in ITIL, further investigation is required into these unmatched control objectives and their requirements, including how they relate to each other.

4 RELATIONSHIPS BETWEEN UNMATCHED CONTROL OBJECTIVES AND CRYPTOGRAPHY

Each unmatched control objective is related to cryptography through the use of a policy requiring cryptographic keys and digital certificates. Below are the measures required to satisfy the five cryptographic control objectives as extracted from DS5:

Table 1. Measures required by unmatched control objectives

Control Objectives	Required Measures
Counterparty Trust (Objective 5.13)	Organisational policy
Transaction Authorisation (Objective 5.14)	Organisational policy
Non-repudiation (Objective 5.15)	Organisational policy
Trusted Path (Objective 5.16)	Organisational policy
Cryptographic Key Management (Objective 5.18)	Cryptographic procedures and protocols

As this paper focuses primarily on management as opposed to operations and administration, only the management measures are mentioned. The above measures need to be implemented through the use of cryptographic mechanisms (hardware or software systems) that are able to perform the necessary cryptographic functions.

The COBIT DS5 control objectives 5.13, 5.14, 5.15 and 5.16 are generally found together and have a “joint existence”. An example of where this joint existence can be found is in an electronic financial transfer or exchange of sensitive information. Both parties involved in such a transaction would require the authenticity of each other’s identity (Counterparty Trust). The transfer to be performed must be permitted (Transaction Authorisation) and may be done over a secure medium (Trusted Path). In the case of a financial transaction, some measure needs to be in place to prevent the repudiation of the transaction (Non-repudiation).

When using cryptography, a transaction’s integrity and confidentiality are automatically provided, as the result of the encryption process (cipher text) is not readily readable and cannot be tampered with as the decryption process will fail. The author terms this as the “side effect” of cryptography. This holds as long as the encryption/decryption keys are not compromised (RSA Professional Services, 2003). Public key infrastructure (PKI) makes use of symmetric and asymmetric encryption and consists of a set of policies, procedures and services to support applications of public key cryptography (National Security Agency, 2002). From the previous statements and the requirements from table 1, it is clear that PKI may be used as the measure to meet the unmatched control objectives.

An important discovery here is that the Cryptographic Key Management objective (Control Objective 5.18) must be in place before any of the other control objectives can be implemented, as this control objective is responsible for the management of cryptographic keys used by technical measures addressing the other control objectives. This creates a dependency amongst the control objectives as shown in figure 4.

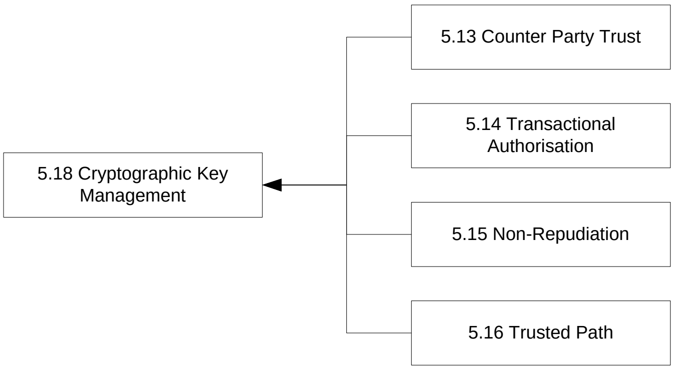

5.13 Counter Party Trust
5.14 Transactional Authorisation
5.18 Cryptographic Key Management
5.15 Non-Repudiation
5.16 Trusted Path

Figure 4. COBIT DS5 cryptographic dependency

Given the joint existence of the above control objectives and the side effect of cryptography, implementing PKI to address the Cryptographic Key Management will also indirectly satisfy the remaining unmatched control objectives. Therefore a framework or model using PKI is required to fill the gap found in ITIL.

This framework or model needs to be generic in nature and not specific to a certain methodology or product. Special interest needs to be placed on the security policies regarding the various aspects of PKI which include encryption/decryption, key management, certificate management, identities, protocols and procedures. A number of frameworks (NIST, 2003) and models (KPMG, 2002) were found and for the purposes of this paper the Information Assurance Technical Framework was chosen, as it was the most generic.

5 THE INFORMATION ASSURANCE TECHNICAL FRAMEWORK

The Information Assurance Technical Framework (IATF) Release 3.1 was developed by the National Security Agency (NSA) to provide technical guidance for protecting information and information infrastructures (NSA, 2002). The IATF defines a process for developing a system with information assurance and the security requirements for the hardware and software components in this system providing guidance to a wide audience ranging from federal agencies to commercial organisations.

Of interest to this paper is Chapter 8 which covers PKI in detail. It is important to note that PKI does not address the specific security requirements of organisations and forms the building blocks used by other security technologies (NSA, 2002). PKI has processes and services that manage keys and certificates provided to cryptographic mechanisms for authentication and encryption, making it an enabler rather than a solution.

IATF Chapter 8 focuses on four essential services provided by PKI supporting infrastructure and applications using cryptography. These four services are:

- *Certificate (Public Key) Management* – Asymmetric cryptography employs digital certificates which bind a set of public/private keys to a particular identity.
- *Symmetric Key Management* – This is the process in which a central entity generates, distributes and manages a secret key for multiple recipients.
- *Infrastructure Directory Service* – Directory service, through the use of servers, provides access to public information such as public certificates, infrastructure certificates and compromised key information within the PKI.
- *Infrastructure Management* – This service involves the management of the infrastructure itself.

The above four services are supported by processes that perform independent tasks but are all related. Each of the four services provided by PKI are the main measures. The term ‘main’ is used because they are not the only measures that exist in this context. Each service in itself contains measures that make up the service (the subprocesses). Each subprocess is not considered to be a measure in this context, as together they provide the building blocks of the services as shown in figure 5.

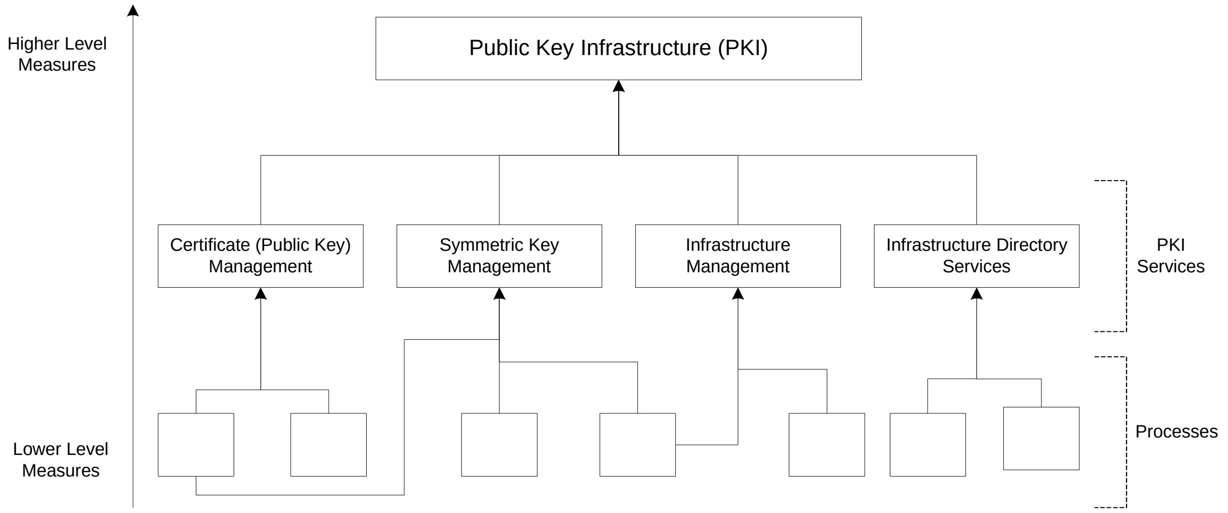

Higher Level Measures
Public Key Infrastructure (PKI)
Certificate (Public Key) Management
Symmetric Key Management
Infrastructure Management
Infrastructure Directory Services
PKI Services
Processes
Lower Level Measures

Figure 5. Structure of measures in PKI

Much like COBIT and ITIL, it is necessary to extract the measures from the IATF Chapter 8 and map them to COBIT DS5 and ITIL Security Management.

6 IATF CHAPTER 8 AND COBIT DS5

Having identified PKI as a measure, it is necessary to connect it to the unmatched control objectives. Using a matrix similar to the one used for mapping ITIL security measures to COBIT DS5 determines how PKI maps onto COBIT DS5. There are two types of cells within the matrix:

- An *X cell* indicates a mapping.
- A *blank cell* indicates no mapping.

Table 2. Matrix between COBIT unmatched control objectives and IATF Chapter 8 PKI (direct mapping)

COBIT Unmatched Control Objectives	IATF PKI
5.12 Counterparty Trust	
5.14 Transaction Authorisation	
5.15 Non-repudiation	
5.16 Trusted Path	
5.18 Cryptographic Key Management	**X**

From the above matrix it is possible to see the *direct* relationship between the PKI as a whole and the unmatched COBIT objectives. Taking into account the side effect of cryptography, an indirect mapping between IATF Chapter 8 and COBIT DS5 is possible as shown in figure 6.

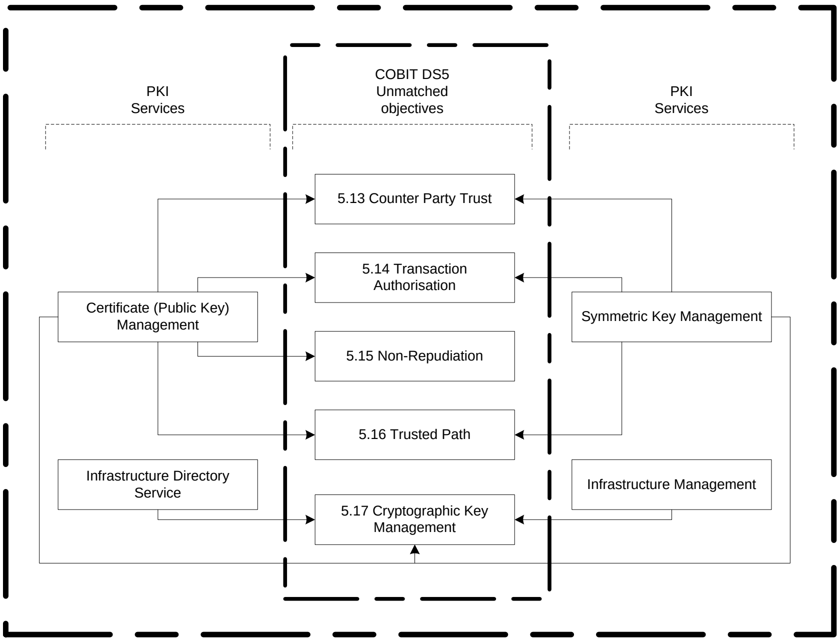

PKI
Services
COBIT DS5
Unmatched
objectives
PKI
Services
5.13 Counter Party Trust
5.14 Transaction Authorisation
Certificate (Public Key) Management
Symmetric Key Management
5.15 Non-Repudiation
5.16 Trusted Path
Infrastructure Directory Service
Infrastructure Management
5.17 Cryptographic Key Management

Figure 6. PKI services connecting to COBIT unmatched control objectives (indirect mapping); viewed as a pyramid looking from the top (refer to figure 1)

With the above mappings (direct and indirect) showing that IATF Chapter 8 can be used to cover cryptography in COBIT DS5, it is necessary to attempt to integrate IATF Chapter 8 into ITIL Security Management. This integration will allow an organisation to implement IATF Chapter 8 following the ITIL processes. It should be kept in mind that IATF Chapter 8 is no “silver bullet” but rather a feasible solution where none has been found.

7 IATF CHAPTER 8 AND ITIL

Given the above nature of PKI, PKI cannot simply be inserted as a measure into the security management component. The reason for this is that ITIL is process-based and PKI is not a process in itself but consists of services made of sub-processes. It is these sub-processes that need to be inserted into ITIL Security Management.

After reviewing the ITIL Security Management processes, it was determined that the *Implement* activity would be the most appropriate place to insert the IATF Chapter 8 sub-processes. Within the Implement activity, the ITIL measures are categorised under the following headings:

- Asset Classification and Control
- Personnel Security
- Communication and Operations Management
- Access Control

Below is a table matrix that maps the IATF processes into the ITIL *Implement* activity. There are two types of cells within the matrix:

- An *X cell* indicates a mapping.
- A *blank cell* indicates no mapping.

Table 3. Mapping matrix between IATF processes and ITIL Implement activity

IATF Chapter 8 Subprocesses	**ITIL Security Process Implement Activity**			
	Asset Classification and Control	Personnel Security	Communication and Operations Management	Access Control
Administration	**X**		**X**	
Registration		**X**		**X**
Policy Creation			**X**	
Ordering			**X**	
Key Generation			**X**	
Certificate Generation			**X**	
Rekey			**X**	
Destruction			**X**	
Accounting	**X**		**X**	
Compromise Recovery			**X**	
Distribution			**X**	

Table 3 shows the complex nature between the IATF Chapter 8 processes and the *Implement* activity. It is not a one-to-one relationship in which a single process is placed under a single heading. Some of the IATF Chapter 8 processes can be classified under more than one category within the *Implement* activity.

By examining the interaction of the PKI services with the PKI processes, it was possible to extend the IATF Chapter 8 mapping further to include other processes within ITIL Security Management as shown in figure 7.

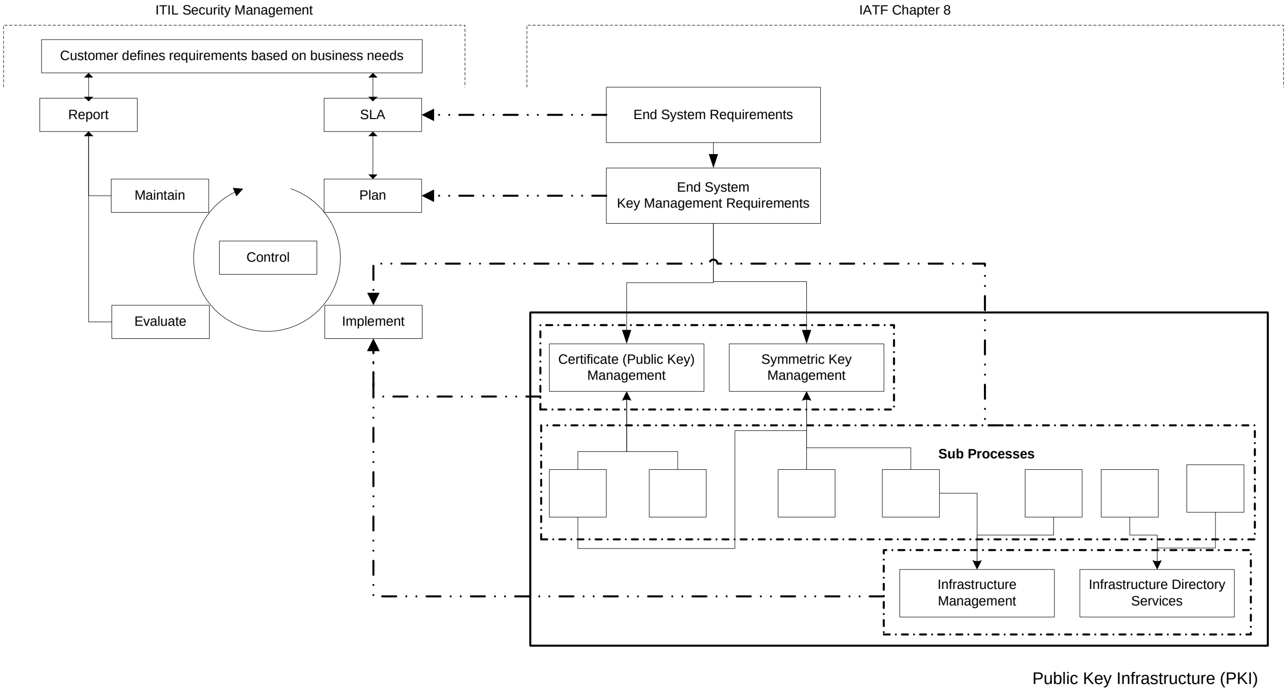

ITIL Security Management
IATF Chapter 8
Customer defines requirements based on business needs
Report
SLA
End System Requirements
Maintain
Plan
End System
Key Management Requirements
Control
Evaluate
Implement
Certificate (Public Key) Management
Symmetric Key Management
Sub Processes
Infrastructure Management
Infrastructure Directory Services
Public Key Infrastructure (PKI)

Figure 7. Complete mapping between IATF Chapter 8 and ITIL Security Management

The IATF Chapter 8 follows a similar path when determining the security requirements. Initially the *End Systems Requirements* for cryptography are chosen and converted into the *End System Key Management Requirements.* These two activities are cleanly mapped into the ITIL Security Management processes as shown in figure 7. The four PKI services connect to the *Implement* activity as they are the by-product of implementing the PKI processes.

8 CONCLUSION

This paper focused on two major frameworks within the IT industry and how they relate to each other from a security perspective. Both frameworks were mapped against each other to determine their relationship and the shortfalls were investigated, providing some insight as to how these frameworks operate at different levels within an organisation.

The mapping shown in figure 7 addresses the cryptography shortfall found in ITIL Security Management and IATF PKI has been proven to comply with COBIT DS5. This mapping will give rise to a model that will provide a more complete mapping between ITIL and COBIT security through the integration of IATF Chapter 8 into ITIL Security Management. An organisation implementing ITIL and COBIT will be able to utilise this model to measure the compliance of ITIL with COBIT DS5. The author of this paper is currently developing this model as part of a research study and it will be made publicly available at its completion.

The processes followed in mapping ITIL to COBIT including the mapping of IATF Chapter 8 to COBIT and ITIL have illustrated that there is no single framework to deal with every aspect of IT. Each framework has been developed with a specific goal in mind and an organisation wanting to address IT will probably have to use more than one framework to get the job done. This reinforces the saying that there is no silver bullet (Gillen, 2004; Computer Times, 2004; Earles, 2000; Ashford, 2005). IT practitioners, IT management and executives should take this into account when dealing with IT within their organisation.

This paper focused solely on the security aspects of the framework, but the research methodology used can be applied to other areas of IT to find relationships that may exist between other frameworks that operate at the same or at a different level. Of particular interest was the discovery of a hierarchical structure of the unmatched control objectives creating dependencies of control objectives. This notion of dependency can be extended further to address all the objectives of DS5 and COBIT as a whole, which could lead to COBIT being viewed in a new light.

REFERENCES

1. IT Governance Institute (2000). *COBIT 3rd Edition, Control Objectives*. USA: ISACF
2. OGC (2002). *Best Practice for Security Management*. UK: The Stationary Office
3. Rudd, C. (2004). *An Introductory Overview of ITIL*. UK: itSMF
4. National Security Agency (2002). *Information Assurance Technical Framework*. Available WWW: http://www.iatf.net/framework_docs/version-3_1/index.cfm (Accessed 19 January 2005)
5. Spafford, G & Gene, K. (2004). *Top ITIL Myths*. Available WWW: http://itmanagement.earthweb.com/service/article.php/3295251 (Accessed 13 April 2005)
6. Williams, P. (2002). *Value versus cost: governing IT on a reduced budget*. Available WWW: http://www.computerweekly.com/articles/article.asp?liArticleID=109833&liFlavourID=1 (Accessed 17 April 2005)
7. RSA Professional Services. (2003). Digital *Certificate Management: Navigating your success*. Available WWW: http://www.rsasecurity.com/support/impguides/index.asp (Accessed 29 January 2005)
8. Ashford, W. (2005). *ITIL 'needs team support'*. Available WWW: http://www.itweb.co.za/sections/enterprise/2005/0504061020.asp?S=Enterprise%20Solutions&A=ENS&O=FRGN (Accessed 10 April 2005)
9. Earls, J. (2000). *Frameworks! Make room for another Silver Bullet*. Available WWW: http://www.cbd-hq.com/articles/2000/000301je_frameworks.asp (Accessed 17 April 2005)
10. Gillen, N. (2004). *Software's Silver Bullet?*. Available WWW: http://www.nextgenerationservices.com/document.asp?doc_id=49917&site=boardwatch (Accessed 17 April 2005)
11. Computer Times. (2004). *No Silver Bullet*. Available WWW: http://it.asia1.com.sg/specials/spotlights20040616_002.html (Accessed 3 April 2005)

12. NIST. (2003). *Key Management Project Part 1*. Available WWW: http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf (Accessed 25 March 2005)

13. NIST. (2003). *Key Management Project Part 2*. Available WWW: http://csrc.nist.gov/CryptoToolkit/kms/guideline-2-Jan03.pdf (Accessed 25 March 2005)

14. NIST. (2003). *Key Management Project Part 3*. Available WWW: http://csrc.nist.gov/CryptoToolkit/kms/key-management-guideline-(workshop).pdf (Accessed 25 March 2005)

15. KPMG. (2002). *Key Management Policy and Practice Framework.* Available WWW: http://www.ncipher.com/insights/km/km_kpmg_intro.html (Accessed 29 March 2005)

16. IT Governance Institute. (2004). *COBIT Mapping*. Available WWW: http://www.itgi.org (Accessed 7 June 2004)

17. John Morency. (2005). *Best practice, practice, practice*. Network World, Vol. 22, Iss. 1; pg. 37