

AN OVERVIEW OF INFORMATION SECURITY STANDARDS

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Introduction.....	3
II. Standards for Information Security	4
ISO Standards	4
Payment Card Industry Data Security Standard.....	8
COBIT.....	8
ITIL (or ISO/IEC 20000 series)	9
III. Regulations Related to Information Security	11
SOX.....	11
COSO	12
HIPAA	13
FISMA	14
FIPS.....	14
Regulations in Hong Kong.....	15
IV. Implementation	17
V. Conclusion	18

SUMMARY

Information security plays an important role in protecting the assets of an organisation. As no single formula can guarantee 100% security, there is a need for a set of benchmarks or standards to help ensure an adequate level of security is attained, resources are used efficiently, and the best security practices are adopted. In this paper, we give a brief introduction to the various standards and regulations that are available for information security, including ISO standards, COBIT, the Sarbanes-Oxley Act, and so on.

I. INTRODUCTION

While information security plays an important role in protecting the data and assets of an organisation, we often hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organisations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both government¹ and business².

To address the situation, a number of governments and organisations have set up benchmarks, standards and in some cases, legal regulations on information security to help ensure an adequate level of security is maintained, resources are used in the right way, and the best security practices are adopted. Some industries, such as banking, are regulated, and the guidelines or best practices put together as part of those regulations often become a *de facto* standard among members of these industries.

In this paper, we give a brief introduction to the most commonly adopted standards and regulations for information security.

¹ <http://www.networkworld.com/news/2006/030706-government-cio-survey.html>

²

http://www.deloitte.com/dtt/press_release/0,1014,sid%253D1000%2526cid%253D171269,00.html

II. STANDARDS FOR INFORMATION SECURITY

This section introduces the various standards for information security.

ISO STANDARDS

The International Organisation for Standardisation (ISO), established in 1947, is a non-governmental international body that collaborates with the International Electrotechnical Commission (IEC)³ and the International Telecommunication Union (ITU)⁴ on information and communications technology (ICT) standards⁵. The following are commonly referenced ISO security standards:

1. ISO/IEC 27002:2005 (Code of Practice for Information Security Management)

ISO/IEC 27002:2005 (replaced ISO/IEC 17799:2005 in April 2007⁶) is an international standard that originated from the BS7799-1, one that was originally laid down by the British Standards Institute (BSI). ISO/IEC 27002:2005 refers to a code of practice for information security management, and is intended as a common basis and practical guideline for developing organisational security standards and effective management practices⁷.

³ <http://www.iec.ch/>

⁴ <http://www.itu.int/net/home/index.aspx>

⁵ http://www.iso.org/iso/iso_catalogue/faq_standards_2.htm

⁶ http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

⁷ http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

This standard contains guidelines and best practices recommendations for these 10 security domains: (a) security policy; (b) organisation of information security; (c) asset management; (d) human resources security; (e) physical and environmental security; (f) communications and operations management; (g) access control; (h) information systems acquisition, development and maintenance; (i) information security incident management; (j) business continuity management; and (k) compliance.

Among these 10 security domains, a total of 39 control objectives and hundreds of best-practice information security control measures are recommended for organisations to satisfy the control objectives and protect information assets against threats to confidentiality, integrity and availability⁸.

2. ISO/IEC 27001:2005 (Information Security Management System - Requirements)

The international standard ISO/IEC 27001:2005 has its roots in the technical content derived from BSI standard BS7799 Part 2:2002. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organisation. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets⁹. This standard is usually applicable to all types of organisations, including business enterprises, government agencies, and so on.

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

⁸ <http://www.iso27001security.com/html/27002.html>

⁹ http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

- a) “Plan” phase – establishing the ISMS
- b) “Do” phase – implementing and operating the ISMS
- c) “Check” phase – monitoring and reviewing the ISMS
- d) “Act” phase – maintaining and improving the ISMS

Often, ISO/IEC 27001:2005 is implemented together with ISO/IEC 27002:2005. ISO/IEC 27001 defines the requirements for ISMS, and uses ISO/IEC 27002 to outline the most suitable information security controls within the ISMS¹⁰.

ISO/IEC 27002 is a code of practice that provides suggested controls that an organisation can adopt to address information security risks. These controls are not mandatory. There is therefore no certification for ISO/IEC 27002, but a company can be certified compliant with ISO/IEC 27001 if the management process follows the ISMS standard. There is a list of accredited certification bodies that can certify an organisation against the ISMS standard, which is maintained on the UK Accreditation Service website¹¹.

3. ISO/IEC 15408 (Evaluation Criteria for IT Security)

The international standard ISO/IEC 15408 is commonly known as the “Common Criteria” (CC)¹². It consists of three parts: ISO/IEC 15408-1:2005 (introduction and general model), ISO/IEC 15408-2:2005 (security functional requirements) and ISO/IEC 15408-3:2005 (security assurance requirements). This standard helps evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard.

Hardware and software can be evaluated against CC requirements in accredited testing laboratories to certify the exact EAL (Evaluation Assurance Level) the

¹⁰ <http://www.iso27001security.com/html/27002.html#RelationTo27001>

¹¹ http://www.ukas.com/about_accreditation/accredited_bodies/certification_body_schedules.asp

¹² http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm

product or system can attain. There are 7 EALs: EAL1 - Functionally tested, EAL2 - Structurally tested, EAL3 - Methodically tested and checked, EAL4 - Methodically designed, tested and reviewed, EAL5 - Semi-formally designed and tested, EAL6 - Semi-formally verified, designed and tested, and EAL7 - Formally verified, designed and tested. A list of accredited laboratories as well as a list of evaluated products can be found on the Common Criteria portal¹³. The list of products validated in the USA can be found on web-site of the Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS)¹⁴.

4. ISO/IEC 13335 (IT Security Management)¹⁵

ISO/IEC 13335 was initially a Technical Report (TR) before becoming a full ISO/IEC standard. It consists of a series of guidelines for technical security control measures:

- a) ISO/IEC 13335-1:2004 documents the concepts and models for information and communications technology security management.
- b) ISO/IEC TR 13335-3:1998 documents the techniques for the management of IT security. This is under review and may be superseded by ISO/IEC 27005.
- c) ISO/IEC TR 13335-4:2000 covers the selection of safeguards (i.e. technical security controls). This is under review and may be superseded by ISO/IEC 27005.
- d) ISO/IEC TR 13335-5:2001 covers management guidance on network security. This is also under review, and may be merged into ISO/IEC 18028-1, and ISO/IEC 27033.

¹³ <http://www.commoncriteriaportal.org/public/consumer/>

¹⁴ <http://niap.bahialab.com/cc-scheme/vpl/>

¹⁵ <http://www.iso27001security.com/html/others.html>

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The Payment Card Industry (PCI) Data Security Standard (DSS)¹⁶ was developed by a number of major credit card companies (including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International) as members of the PCI Standards Council to enhance payment account data security. The standard consists of 12 core requirements, which include security management, policies, procedures, network architecture, software design and other critical measures. These requirements are organised into the following areas:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

COBIT

The Control Objectives for Information and related Technology (COBIT) is *“a control framework that links IT initiatives to business requirements, organises IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and*

¹⁶ <https://www.pcisecuritystandards.org/tech/index.htm>

*defines the management control objectives to be considered*¹⁷. The IT GOVERNANCE INSTITUTE (ITGI) first released it in 1995, and the latest update is version 4.1, published in 2007.

COBIT 4.1 consists of 7 sections, which are (1) Executive overview, (2) COBIT framework, (3) Plan and Organise, (4) Acquire and Implement, (5) Deliver and Support, (6) Monitor and Evaluate, and (7) Appendices, including a glossary. Its core content can be divided according to the 34 IT processes.

COBIT is increasingly accepted internationally as a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks. Based on COBIT 4.1, the COBIT Security Baseline focuses on the specific risks around IT security in a way that is simple to follow and implement for small and large organisations. COBIT can be found at ITGI¹⁸ or the Information Systems Audit and Control Association (ISACA)¹⁹ websites.

ITIL (OR ISO/IEC 20000 SERIES)

The Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management (ITSM), and focuses on the service processes of IT and considers the central role of the user. It was developed by the United Kingdom's Office

¹⁷

http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Co biT4.1_Brochure.pdf

¹⁸ <http://www.itgi.org>

¹⁹ <http://www.isaca.org/bookstore>

of Government Commerce (OGC)²⁰. Since 2005, ITIL has evolved into ISO/IEC 20000²¹, which is an international standard within ITSM.

An ITIL service management self-assessment can be conducted with the help of an online questionnaire²² maintained on the website of the IT Service Management Forum. The self-assessment questionnaire helps evaluate the following management areas: (a) Service Level Management, (b) Financial Management, (c) Capacity Management, (d) Service Continuity Management, (e) Availability Management, (f) Service Desk, (g) Incident Management, (h) Problem Management, (i) Configuration Management, (j) Change Management, and (k) Release Management.

²⁰ http://www.ogc.gov.uk/guidance_itsm_4438.asp

²¹

<http://www.iso.org/iso/search.htm?qt=20000&searchSubmit=Search&sort=rel&type=simple&published=true>

²² <http://www.itsmf.com/bestpractice/selfassessment.asp>

III. REGULATIONS RELATED TO INFORMATION SECURITY

In addition to the various industry standards bodies and guidelines, certain regulated businesses, such as banking, may need to observe the regulations and guidelines specified by their own industry or professional regulatory bodies. In this section, we briefly discuss the US regulations SOX, COSO, HIPAA, and FISMA, and regulations that apply in Hong Kong.

SOX

After a number of high profile business scandals in the US, including Enron and WorldCom, the Sarbanes-Oxley Act of 2002 (SOX) was enacted as legislation in 2002. This act is also known as the “Public Company Accounting Reform and Investor Protection Act”. The purpose is to “*protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes*”²³. This regulation affects all companies listed on stock exchanges in the US.

In section 404, the SOX requires “*each annual report ... contain an internal control report ... [that] contains an assessment of ... the effectiveness of the internal control structures and procedures of the issuer for financial reporting*”. As information technology plays a major role in the financial reporting process, IT controls would need to be assessed to see if they fully satisfy this SOX requirement.

²³ http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf

Although information security requirements have not been specified directly in the Act, there would be no way a financial system could continue to provide reliable financial information, whether due to possible unauthorised transactions or manipulation of numbers, without appropriate security measures and controls in place. SOX requirements indirectly compel management to consider information security controls on systems across the organisation in order to comply with SOX²⁴.

COSO

The COSO (Committee Of Sponsoring Organisations of the Treadway Commission) framework is a framework that initiates an integrated process of internal controls. It helps improve ways of controlling enterprises by evaluating the effectiveness of internal controls. It contains five components²⁵:

1. Control Environment, including factors like integrity of people within the organisation and management authority and responsibilities;
2. Risk Assessment, aiming to identify and evaluate the risks to the business;
3. Control Activities, including the policies and procedures for the organisation;
4. Information and Communication, including identification of critical information to the business and communication channels for delivering control measures from management to staff;
5. Monitoring, including the process used to monitor and assess the quality of all internal control systems over time.

²⁴ http://www.sans.org/reading_room/whitepapers/legal/1426.php

²⁵ http://www.coso.org/publications/executive_summary_integrated_framework.htm

The COSO framework and the COBIT framework described above are both used to satisfy compliance with SOX.

HIPAA

The Health Insurance Portability And Accountability Act (HIPAA) of 1996 is a US law designed to improve the portability and continuity of health insurance coverage in both the group and individual markets, and to combat waste, fraud, and abuse in health insurance and health care delivery as well as other purposes²⁶. The Act defines security standards for healthcare information, and it takes into account a number of factors including the technical capabilities of record systems used to maintain health information, the cost of security measures, the need for training personnel, the value of audit trails in computerised record systems, and the needs and capabilities of small healthcare providers.

A person who maintains or transmits health information is required to maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of that information. In addition, the information should be properly protected from threats to the security and integrity of that information, unauthorised uses, or unauthorised disclosure.

The full set of rules regarding adoption of the HIPAA standards for the security of electronic health information²⁷ and privacy of personal health information²⁸ can be found in US Department of Health and Human Services website.

²⁶ <http://aspe.hhs.gov/admsimp/pl104191.htm>

²⁷ http://www.cms.hhs.gov/SecurityStandard/02_Regulations.asp#TopOfPage

FISMA

FISMA stands for Federal Information Security Management Act, and is a part of the US E-Government Act (Public Law 107-347) that became legislation in 2002²⁹. It requires US federal agencies to develop, document, and implement an agency-wide programme to provide information security for the information (and information systems) that support the operations and assets of the agency. Some of the requirements include:

1. Periodic risk assessments of information and information systems that support the operations and assets of the organisation
2. Risk-based policies and procedures designed to reduce information security risks to an acceptable level
3. Plans for providing adequate security for networks and information systems
4. Security awareness training to all personnel, including contractors
5. Periodic evaluation and testing of the effectiveness of the security policies, procedures and controls. The frequency should not be less than annually. Remedial action to address any deficiencies found to be properly managed.
6. A working and tested security incident handling procedure
7. A business continuity plan in place to support the operation of the organisation.

FIPS

²⁸ <http://www.hhs.gov/ocr/hipaa/finalreg.html>

²⁹ <http://csrc.nist.gov/groups/SMA/fisma/overview.html>

The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is an official series of publications relating to standards and guidelines adopted and made available under the provisions of the FISMA³⁰. FIPS Publication 199, *Standards for Security Categorisation of Federal Information and Information Systems*, is the first mandatory security standard laid down under the FISMA legislation. FIPS Publication 200, entitled “*Minimum Security Requirements for Federal Information and Information Systems*” is the second mandatory set of security standards that specify minimum security requirements for US federal information and information systems across 17 security-related areas. US federal agencies must meet the minimum security requirements defined in this standard by selecting appropriate security controls and assurance requirements laid down in NIST Special Publication 800-53 (*Recommended Security Controls for Federal Information Systems*).

The 17 security-related areas include: (a) access control; (b) awareness and training; (c) audit and accountability; (d) certification, accreditation, and security assessments; (e) configuration management; (f) contingency planning; (g) identification and authentication; (h) incident response; (i) maintenance; (j) media protection; (k) physical and environmental protection; (l) planning; (m) personnel security; (n) risk assessment; (o) systems and services acquisition; (p) system and communications protection; and (q) system and information integrity.

REGULATIONS IN HONG KONG

In Hong Kong, there are currently no regulations similar to that of the SOX. Nevertheless, the Government of the HKSAR has issued a *Baseline IT Security Policy* and a series of guidelines related to IT security that provide references and guidance to Government

³⁰ <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

bureaux and departments on the protection of Government information systems. Documents relating to this are also published on the government website³¹ for public reference.

In addition, a variety of industry regulatory bodies in Hong Kong have laid down requirements on security controls and governance on IT systems for their members. As an example, the Hong Kong Monetary Authority has established guidelines for electronic banking services. The document “*TM-E-1 Supervision of E-banking*”³² sets out the approach and general principles for risk management with regard to e-banking. It covers topics on board- and senior-management oversight, major technology-related controls relevant to e-banking, and customer security.

³¹ <http://www.ogcio.gov.hk/eng/prodev/esecpol.htm>

³² <http://www.info.gov.hk/hkma/eng/bank/spma/attach/TM-E-1.pdf>

IV. IMPLEMENTATION

Although there are a number of standards on information security available now, these standards are often general guidelines or principles that may not all be applicable to a particular organisation.

If an organisation aims to implement security controls that are in compliance with a particular standard, or even a set of standards, a concerted effort from top management down to end-users would be required as part of the development and implementation process. Care must be taken to ensure that standardised policies or guidelines are applicable to, and practical for, that particular organisation's culture, business and operational practices.

The organisation should first perform a "gap analysis" to identify the current security controls within the organisation, the potential problems and issues, the costs and benefits, the operational impact, and the proposed recommendations before applying any chosen standards. The creation of security policies and guidelines should only follow the completion of a gap analysis. Management support is necessary at all levels. User awareness programmes should also be conducted to ensure that all employees understand the benefits and impacts before the deployment of new security policies and guidelines.

A common problem that crops up after implementation of a standardisation exercise is an increase in the number of complaints received from users of IT services due to the restrictions imposed by new security controls. The successful implementation of any information security standards or controls must be a balance of security requirements, functional requirements and user requirements.

V. CONCLUSION

Although there are a number of information security standards available, an organisation can only benefit if those standards are implemented properly. Security is something that all parties should be involved in. Senior management, information security practitioners, IT professionals and users all have a role to play in securing the assets of an organisation. The success of information security can only be achieved by full cooperation at all levels of an organisation, both inside and outside.