7 Information Security Management

7.1 Suggested Discussion Points for Exercises

1. Exercise: At a high level view COBIT, ITIL and ISO27002 have a lot in common. However, each of the security and control frameworks discussed in this unit has its unique characteristics. Identify and discuss similarities existing between these frameworks. Summarise and discuss with your colleagues specific differences between them. The following categories may help in your comparative analysis of the frameworks: *technology, implementation, environment, personnel, controls, processes and metrics*.

Discussion is based upon the section **Frameworks for Control and Security: COBIT®, ITIL®, and ISO 27002**:

Over the years three rather different, but widely accepted, IT governance frameworks have been developed. They are COBIT®, ITIL® and ISO 27002. Each of these frameworks was developed in a different country and by a third party, i.e. these frameworks are vendor-independent. Although any of these frameworks may not serve as a silver bullet to resolving information security risks, each has its fortes in IT governance.

Control Objectives for Information and related Technology, or COBIT® is increasingly popular framework of practices for IT, internal information controls and risks mitigation. COBIT, developed by America's IT Governance Institute, aims to facilitate implementation of enterprise-wide governance of IT. Its objective is to help enterprises to integrate information technology with business objectives and strategic management, to harvest value of their information assets and capitalise on IT in an increasingly competitive business and stringent regulatory environments. COBIT is a process oriented framework, which provides management guidelines for monitoring and evaluating an enterprise's IT resources. The framework offers tools responsive to the management needs to control and monitor enterprise's IT capability for its various business processes. The best practice approach provided by COBIT includes such tools as:

- Performance drivers for IT
- Best practices for IT processes and relevant critical success factors
- Elements for performance outcome measurement
- Maturity models instrumental for decision making over capability improvements.

According to COBIT there are 34 IT processes in an enterprise, every process is assigned a level of maturity on a scale of 0–5 from non-existent to optimised or best practice. The maturity levels are used for benchmarking of IT capabilities. IT processes are grouped into four domains, such as:

- Plan and Organise;
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate.

For each COBIT process a set of control objectives is assigned. For instance, a process *Ensure System Security* which belongs to the domain of *Delivery and Support* will have an objective of *Minimise the impact of security vulnerabilities and incidents*. This objective can be assessed by the number and severity of projected and actual information security breaches, % of compromised cryptographic keys compromised and revoked, number of access rights authorised, revoked, changed, etc. Table 1 summarises selected processes and general control objectives outlined in the COBIT framework.

Domain	High Level Control Objectives
Delivery and Support	Ensure Continuous Service
	Ensure System Security
	Educate and Train Users
	Manage Service Desk and Incidents
	Manage Problems
Monitor and Evaluate	Monitor and Evaluate IT Processes
	Monitor and Evaluate Internal Control Systems
	Ensure Regulatory Compliance
	Provide IT Governance

Table 1 Selected Control Objectives in COBIT.

COBIT takes a best-practice approach to assist managers in establishing appropriate internal controls and aligning control needs, business risks and IT capabilities. The framework ensures that internal control systems support the enterprise's business processes through identification and measurement of individual control activities. These activities comprise of management policies/procedures, business practices and organisational structures.

In addition to other risks that an enterprise can face, COBIT deals with IT security. COBIT Security Baseline comprehensively covers risks of IT security and provides key controls for mitigating technical security risks. As discussed earlier in the unit enterprises, especially trading in the US, have to comply with stringent regulations. COBIT has established itself as the most adopted internal control framework to achieve compliance with the Sarbanes-Oxley Act.

ISO27002: Code of Practice for Information Security Management.

ISO 27002, the updated version of ISO 17799 in 2007, is a *Code of practice for information security management*. It provides the general principles for planning, implementing and improving information security management for businesses. The standard, released by the International Standards Organisation in Geneva, establishes the guidelines on information security control objectives and focuses on information in its various forms.

It is worth mentioning that ISO 27002 addresses security of information in possibly all of its formats including electronic files, paper documents, recordings/media and communications. The standard is comprehensive enough to group information in context of communication into conversations (telephone, mobile, face to face) and messages (email, fax, video and instant messaging).

ISO 27002 suggests initiating implementation of information security management by gathering company's information security requirements. This is done through a process consisting of the following steps:

1. **Perform risk assessment** – aimed at identifying vulnerabilities and threats, as well as establishing their likelihood of them causing an information security breach and its consequences to business objectives.
2. **Study legal requirements** – this step includes addressing the legislative and contractual requirements of all business stakeholders including suppliers, partners, etc. and ensuring that the regulatory requirements specific to the business are met.
3. **Scrutinise requirements internal to business** – through examination of information management processes, methods and practices inside the organisation it is possible to identify information security needs and requirements unique to the organisation.

Having examined the company's information security needs and requirements, ISO 27002 recommends developing/improving the business's *information security program.* This program is built from the best-practices provided by ISO 27002 by selecting practices which meet information security requirements unique to the company. It is recommended to establish core security practices such as:

- "Allocate responsibility for information security
- Develop an information security policy document
- Make sure applications process information correctly
- Manage information security incidents and improvements
- Establish a technical vulnerability management process
- Provide security training and awareness
- Develop a continuity management process".

The basis of the legal practices in a company's information security program must include at least:

- "Respect intellectual property rights
- Safeguard organisational records
- Protect privacy of personal information" (*ISO 27002: 2005 Introduction)*

ISO 27002 addresses objectives of information security management and recommends controls which should be used to achieve these objectives. For example, the section concerned with *Information Security Incident Management* includes an objective, *Make sure that information system security incidents are promptly reported.* Relevant controls corresponding to this objective will include, *Report information security events using the appropriate management reporting channels* and *Make sure that security events are reported promptly.* In addition to the set of objectives and controls ISO27002 provides notes and guidelines on how to implement controls and apply objectives. For the objective discussed above one of the guidance notes is *Establish a formal information security event reporting procedure.*

The set of best practices comprehensively covers a broad range of management areas from Human Resource Security Management to Information Security Incident Management. Any business organisation is not compelled to implement the entire set of best practices provided in ISO 27002 – only specific practices which help address information security risks or meet a compliance requirement relevant to the organisation need to be applied.

Information Technology Infrastructure Library or ITIL® emerged in recognition to an increasing dependence of enterprises on information and IT in order to meet their business needs. Developed by the UK Office of Government Commerce, ITIL comprises of a comprehensive set of good practice documentation for managing IT infrastructure, development and delivery of quality services. Through the use of best practices ITIL provides a systematic approach to the IT Service Management. ITIL has been highly acclaimed and adopted by such large organisations as Barclays Bank, HSBC, British Airways, MOD, etc.

ITIL has focuses on the Service Management and IT support for operational processes and their continual improvement. Over the years since the earlier versions of ITIL it has emerged that Service Management is a wider concept than just supporting the end-product. The later version (version 3) of ITIL now addresses the Service Lifecycle including Strategy, Design, Transition and Operations.

ITIL covers Security Management as a process of embedding information security into organisational management. ITIL Security Management is largely based on the ISO 17799/ISO 27002 standard and treats information security as the process of safeguarding information from risks. It addresses the need to minimise information security risks, often concentrating on the physical security of information assets, in order to achieve and improve IT service management. Specifically, information security breaches and attacks can negatively impact service operations and continuity thereby in ITIL context, degrade service value and benefit.

Various IT control frameworks have emerged over the past decades, enabling organisations to establish robust internal security controls. Their primary objective is to provide a structured system for any business to establish a system of controls as complete as possible fully addressing corporate business processes and infrastructure. The frameworks described here offer substantially different approaches to control and security. However, they are flexible enough to allow any business, from small companies to global enterprises, to adapt and implement only selected components of the framework to the specific needs of a business.

2. Exercise: Following a number of information security incidents, the UK government conducted a review of its data handling procedures. In a small group, or individually, research some of the news headlines related to data loss incidents. Discuss with your colleagues what security control objectives should be in place to avoid such incidents of data loss in the future.

Compare your suggestions to the information security agenda suggested in the following report **Cabinet Office (2008)** ***Data Handling Procedures in Government: Final Report*** http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx

Finally, what security and control framework(s) are recommended to be implemented by this report?

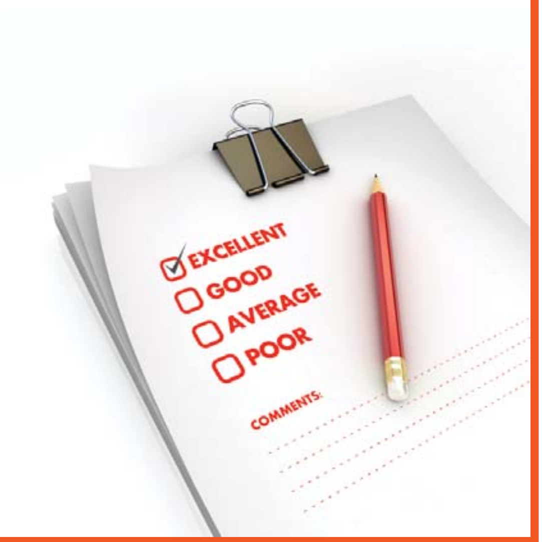
Discussion Points:

The Cabinet Office Report recommends implementation of the following specific measures:

- Regular assessments of information and risks associated with it
- Controlled access to the information infrastructure
- Access to raw data is kept to a minimum
- Clarified ownership of data to contractors and third parties.

Fostering Organisational Culture:

- Strong accountability culture
- Information is seen as a corporate asset
- Staff awareness and education
- Clear expectations and understanding of consequences.



3. Exercise: Research how one of the Fortune 100 companies protects its brand online. Or you may choose one of the following companies:

- Toyota
- Lloyds tsb
- NatWest
- Sony

Identify measures the company of your choice takes to protect and manage its brand online. Collect information about possible threats pertaining to brand that the company experienced in the past.

Also, attempt to list possible benefits and savings obtained through online brand protection. Share your findings with your class colleagues or on the discussion forum as directed by your instructor.

Discussion Points:

You may find it useful to research the cases studies on the Mark Monitors web page. One of the companies mentioned there is Toyota. Brand integrity is of an utmost importance to the company. A proactive approach aimed at preventing, detecting and responding to counterfeit and gray activity on the Internet was taken by Toyota brand management team. As a result Toyota successfully:

- Increased its online brand protection strategy across several countries and avoided overhead costs
- Integrated several of its auction sites thereby reducing the administration costs
- Improved its position in reporting, case history data availability and image protection.

Find more detailed information at: http://www.markmonitor.com/cta/cs-toyota/

- Provided instant access to better evidence including case history data, documents and images

Their online brand protection is implemented as follows:

7.2 External Resources and Links

Attorney General's Office State of Connecticut (2006) *Pfizer Data Breach Letter.* Available at http://www.ct.gov/ag/lib/ag/consumers/pfizerdatabreachletter.pdf
Accessed on 10/06/2008

BSI (2006) *ISO/IEC 18028-1:2006 Information Technology. Security Techniques. IT Network Security. Network Security Managemen*t. London: BSI Publications.

Cabinet Office (2008) *Data Handling Procedures in Government: Final Report*
Available from http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/csia/dhr/dhr080625%20pdf.ashx
Accessed on 10/06/2008

Calder A. and Watkins S.(2005) *IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799* – 3rd Edition, Kogan Page.

Calder A. (2005) *A Business Guide to Information Security.* Kogan Page.

IT Governance Institute (2008) *COBIT 4.1 Executive Summary and Framework.* Available from: http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172

Egan M. and Mather T. (2004) *Executive Guide to Information Security: The Threats, Challenges, and Solution.* Symantec Press.

Haag S., Batzan P., Phillips A. *(2006)* Business Driven Technology. *McGraw-Hill.*

MarkMonitor (2007) Gain *Control Over the Vast Unknown: Curtailing Online Distribution of Counterfeit and Gary Market Goods*. White Paper.

MessageLabs (2008) Message Labs Intelligence: April 2008.
Available from: www.messagelabs.com/mlireport/MLI_Report_April_2008.pdf
Accessed on 10/06/2008

Schneier B.(2006) *Secrets and Lies: Digital Security in a Networked World.* Hungry Minds Inc, US.

Silay J. and Koronios A. (2006) *Information Technology: Security and Risk Management.*
J Wiley

Stationery Office (2007) *Personal Internet Security Report.* London: The Stationery Office. Available from: http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf
Accessed on 10/06/2008

Symantec Corporation (2007) *Symantec Internet Security Threat Report: Trends for January–June 2007*, Vol. 12

Weber Schandwick (2007) *Safeguarding Reputation Survey Results Issue 1: Strategies to Recover Reputation*. Available form: http://164.109.94.76/resources/ws/flash/Safe_Rep_Reputation.pdf
Accessed on 10/06/2008