This article is the final article of a 4-part “Leveraging COBIT to Implement Information Security” series. **Part 1** covered how COBIT® 5 can be used to establish the overall framework for the collaboration of technical standards such as the IT Infrastructure Library (ITIL), ISO/IEC 27001 and SANS Critical Security Controls (SANS Top 20). **Part 2** focused on using COBIT® to implement information security process controls within an ITIL system to provide protection envisaged by SANS Top 20. **Part 3** outlined how to implement the Information Security Management System (ISMS) governance framework and enabling tools to manage the security programme. This article shows how the requirements for certification of the ISMS framework can be satisfied by using the approaches outlined in this 4-part series.

An ISMS can be implemented according to the methods and techniques set out in ISO 27001 simply to obtain the best practice benefits established within the standard. Certification of the ISMS is an optional step designed to allow an organisation to demonstrate to third parties that its ISMS does, in fact, meet these best practices for management of information security.

The story outlined in this series of articles started when the IT operations director of a major Australian utility company contacted the author to discuss how the requirements of ISO 27001, which were a requirement for the organisation, could be met efficiently without imposing high costs on the organisation, particularly with regard to evidence collection and storage. The system that was designed went even further than this and simplified the entire process of certification, making the certification process straightforward for both the organisation's management and the certifiers.

*The story outlined in this series of articles started when the IT operations director of a major Australian utility company contacted the author to discuss how the requirements of ISO 27001...could be met efficiently without imposing high costs on the organisation...*
Figure 1 provides a snapshot of what typical ISO 27001 implementation processes may look like for a specific business process. The certification scope of this organisation had been determined as the core business processes on which the business relied to operate and deliver services to its customers. Within each of these business processes there were, in turn, controls over how information was handled (including both storage and communication). For each business application within the scope of certification, a risk assessment was conducted that established the key risk and controls relevant for that application. On the basis of this risk assessment, management was required to implement and maintain ongoing evidence for the operation of these controls within the application.

The certifiers would go through and sample that, in fact, the controls were in place and effective. Within the certification obtained for this organisation, the certification obtained was for the operation of the management system itself rather than the individual controls. Therefore, the evidence required was that the governance controls (including the ISMS) was operating rather than each of the 133 individual controls. The rationale for this approach was that if these governance controls are working, then this will provide the required assurance that the operational controls being managed by the ISMS will be put in place, managed and monitored accordingly.

In order to anchor the process and establish a basis for referencing control implementation and operation within the ISMS, each manager agreed to and signed an Information Security Agreement (ISA) which contained the relevant controls identified within the ISO 27001 Statement of Applicability (SOA) applicable within their business process. The ISA overview and its role within the operation of the ISMS are depicted in figure 2. In this example, internal audit verifies the operation of the ISAs, although this could be outsourced to a third-party organisation if
the internal audit section did not feel it had the required competencies to assess the controls.

**Figure 2—Operation of the Information Security Agreement Process Within an Organisation**

<table>
<thead>
<tr>
<th>Information Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Security ISA Management, Reporting and Verification Process</strong></td>
</tr>
<tr>
<td><strong>Business Divisions</strong></td>
</tr>
<tr>
<td>Processes to be Maintained → Evidence of Control</td>
</tr>
<tr>
<td>Responsible for maintaining → Agreement to maintain</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
</tr>
<tr>
<td>Information Security Calendar ↓ Information Security Controls Master Plan ↓ Information Security Agreements ISA</td>
</tr>
<tr>
<td>Manages ↓ Defines controls to be maintained ↓ Implements</td>
</tr>
<tr>
<td>Information Security Manager ↓ Authorises ↓ ISA</td>
</tr>
<tr>
<td><strong>Information Technology</strong></td>
</tr>
<tr>
<td>Processes to be Maintained ↓ Evidence of Control</td>
</tr>
<tr>
<td>Responsible for maintaining ↓ Agreement to maintain</td>
</tr>
<tr>
<td>IT Manager ↓ Audits and verifies</td>
</tr>
<tr>
<td><strong>Internal Audit</strong></td>
</tr>
<tr>
<td>Information Security Calendar ↓ ISO 27001 Audit Plan ↓ Schedule of verification activities</td>
</tr>
<tr>
<td>Schedules and updates ↓ Determines</td>
</tr>
<tr>
<td>Internal Audit Manager ↓ Audits and verifies</td>
</tr>
</tbody>
</table>

Source: John Frisken. Reprinted with permission.
In this example, ISO 27002 is used as the control objectives framework; however, conceptually, any other control framework, including COBIT, could be used as long as it was suitable, a judgement that management, IT security and internal audit need to make. Refer to Part 3 for a more in-depth discussion of the ISMS.

During the initial certification meetings, the auditors are likely to focus on the initial risk assessments performed by the organisation and how these have been used to implement treatments for any deficiencies identified during the risk assessment. Following a process similar to that outlined in figure 1, the results should be stored in a manner that can be readily maintained over time, preferably in a simple database application. However, a spreadsheet will suffice during the initial data collection.

The Information Security Controls Master Plan provides the details required for the SOA in the certification process, and in the certification example set out here, the Information Security Controls Master Plan was simply adapted to present the view required by the certifiers.

The Information Security Controls Master Plan is the basis on which the organisation carries out its duty of care to protect information from unauthorised or accidental modification, loss, release, or impact upon the safety and well-being of individuals. The plan outlines the Information Security Programme and how management implements controls in order to ensure:

- The effectiveness and efficiency of services and business operations that rely on information
- The protection of the organisation’s commercial interests and information assets that manage this information

Specifically, information plays a vital role in supporting business processes and customer services, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements. Accordingly, information must be protected to a level commensurate with its value to the organisation as well as any legal requirement.

The Information Security Controls Master Plan describes the broad framework within which all enterprise controls over information are implemented via the ISMS. The starting point for this is the alignment of current practices against existing policies, within a Threat Risk Assessment Matrix (TRAM).

A high-level view of the ISMS is shown in figure 3. This graphic was discussed in more depth in Part 2 of this series. It is shown here since it is important in understanding the various components of the ISMS required to support a certified ISMS. The key area of focus is on the ISMS registers and the ISMS reporting engines, particularly as they link into the wider information flows within the overall organisation. These are briefly discussed here:

**Information security responsibility statements**—Statements embodied within the ISA detailing the roles within the organisation responsible for managing each of the business, IT and information security controls identified as required by the organisation’s risk assessment

**Information security policies and guidelines**—The formalised policies and work instructions developed describing how each of the required controls are required to be implemented and maintained. These are derived from the 15 Information Security Operational Management Statements addressing each of the required ISO 27001 control domains identified within the standard.

**Deviation register**—A record of all approvals granted for exceptions from organisational information security policies

**Corrective action requests**—A record of all identified security control deficiencies identified during the ISMS security review or security incident investigations together with recommended corrective actions

**Security training register**—A listing of all personnel who have undertaken security-related training courses
applicable for their roles and positions in the organisation. This register may be used as the basis for follow-up and review of the efficacy of training conducted.

**Figure 3**—Information Security Management System Operations View

![Information Security Management System Operations View]

Source: John Frisken. Reprinted with permission.

**Figure 4**—Information Security Systems Domain (Expanded View)

![Information Security Systems Domain (Expanded View)]

Source: John Frisken. Reprinted with permission

**Information security work requests**—A register of all requests to perform reviews or undertake work in relation to information security.
to management of information security within the organisation. These are listed on the information security calendar of individuals who are involved in the conduct of the work or review of reports.

**Security incident and event register**—A register of all incidents brought to the attention of information security, details of how the incidents were responded to and recommendations for improvements following post-event briefings.

**Risk and issues register**—Registers for risk and issues noted during reviews or brought to the attention of the information security officer. Issues may start as risk and become issues for treatment, or issues raised could become risk.

**Forum reports**—Each month a report is published and distributed for tabling at the Information Security Forum related to reviews performed, reports issued, risk and issues raised, or security incidents during the past month. These are discussed as a basis for agreeing and confirming the scope of the information security functions operation.

The work flow technologies, calendar management function, and knowledge base for information security are depicted at the bottom, right-hand corner of figure 4. These can take many forms, but workflow automation is an essential concept in the implementation of mature IT service management and ISMS solutions, as is the concept of management of a programme of work. Accordingly, workflow-enabled program and project management systems are seen as the ideal platform for managing the program and automating monthly compliance and key performance indicator (KPI) reporting.

The following activities are envisaged as being supported by the workflow:

- Update of the configuration management database (CMDB) configuration items based on approved change management documentation. This would include secure-build identifiers for server and workstation images, specifications of configuration items (CI) for managed network appliances such as firewalls and routers, and software release versions for applications on each server.
- Processing of requests for new or changed application privileges within the corporate enterprise resource planning (ERP) and other applications. Access privileges may relate to either the application functionality or the underlying database access.
- Update of privileged access to operating systems and utilities
- Notification of high-risk monitoring alerts to permit timely intervention to avert possible attacks or failures
- Notification of changes to secure configurations that have not been authorised. This is achieved by automated examination of all images to an approved image and raising alerts for inconsistencies.
- Notifications where unapproved hardware is attached to the network (approved hardware means recorded within the CMDB)
- Notifications where unapproved software is added to the server
- Notifications where changes are made to configurations of network devices
- Scheduling of regular calendar reviews, meetings or other actions to be initiated and follow-up reminders if action is not completed within specified time frames for each type of action.

Certification by a provider will focus on ensuring that the ISMS is operating and the resulting management capability it provides is starting to be evidenced in the form of better security outcomes for the organisation. Adopting a model like that presented in this series of articles not only makes this process practical, but also provides a rich source of evidence and metadata around security matters that the auditors can use as a basis for issuing their certificate.

In many organisations where multiple certifications are in place, the organisation ought to consider the benefits of integrated certifications using common processes and technologies to manage these. This makes it simpler for individuals who are required to operate more than one certification domain, e.g., quality (ISO 9000), IT service management (ITSM) (ISO 20000), information security (ISO 27001), and risk management (ISO 31000).
In an environment such as health care or banking, all and possibly more standards will be in place. A consistent approach and set of technologies will provide significant cost reductions for the organisation and simplify the process for training of personnel and certification, especially where personnel are involved with operating more than one management system.

Conclusion

COBIT facilitates the development of the governance framework within which the information security function makes assessments around risk and priorities for information security, permitting multiple technical standards to operate within the organisation. In the design of the controls and their embedment within the organisation, COBIT's Responsible, Accountable, Consulted, Informed (RACI) techniques allow for controls to be designed taking into account requirements from multiple standards and implemented within a cohesive framework for ongoing review and enforcement.

This has been a high-level summary of the issues involved in the use of COBIT for implementing information security within an organisation. Review of the entire series (4 articles) is recommended to gain a thorough and holistic view of the concepts.

Author’s Note

This case study has been developed based on a real client situation in Australia. The names of the organisations and some other identifying information have been removed. All material is either owned by Information Systems Group Pty Limited or used with permission.

John Frisken, CISA, CA

Is an information security and application development specialist with a distinguished career in professional practice with Ernst & Young and, subsequently, as founder and owner of the Information Systems Group, an international security consulting, systems integration and secure development company headquartered in Sydney, New South Wales, Australia. Since establishing ISG in 1996, Frisken has overseen the delivery of ISG’s services including ISMS implementation projects for many large public sector, judicial and utility organisations in Australia, and development of complex applications leveraging advanced messaging and secure platform technologies. He is a member of ISACA, the Institute of Chartered Accountants in Australia, and the Australian Information Security Association. Frisken led the adaption of the COBIT framework into the IFAC Delivery and Support Standards which are aimed at explaining the application of the framework within a business context. He currently serves as ISG’s director of professional services.