



# Leveraging ISO 27001 for Your Compliance Requirements

*ISO 27001 brings it all together*

By **MICHAEL BEEKEY**

CTG SECURITY SOLUTIONS

## Introduction

*Almost every organization, regardless of size or industry, deals with constantly changing risk, regulatory, and compliance landscapes. Organizations struggle to ensure that their security and enterprise risk management programs and the associated costs address their multiple compliance requirements, are appropriate to their business, and produce demonstrable results of their effectiveness.*

*ISO/IEC 27001:2005 (ISO 27001) as a security control framework may be the most promising option for organizations today juggling multiple compliance and regulatory requirements while seeking process and performance improvements.*

**A SPECIAL CLIENT REPORT**

---

Copyright ©2008 Client Confidential: A special report for clients only. The material covered in this report is for guidance only. Application and implementation guidelines, advice, and consulting are available.

*Copyright ©2008 Client Confidential: A special report for clients only. The material covered in this report is for guidance only. Application and implementation guidelines, advice, and consulting are available.*

*The adoption of ISO 27001 as a security control framework offers several benefits for executive management and the groups and individuals responsible for risk, security, compliance, and audit.*

ISO 27001 is the management system around ISO/IEC 27002:2005 (ISO 27002), which until recently was commonly known as ISO/IEC 17799:2005. While ISO 27001 is already fairly well known and accepted outside of the United States, it is slowly gaining awareness and acceptance within the U.S.

Implementing ISO 27001 requires an organization to create an Information Security Management System (ISMS). Establishing an ISMS around its information security program enables an organization to use a risk-based approach to identifying and satisfying all compliance requirements, justify the selection and implementation of controls, and provide measurable evidence that the controls are operating effectively.

The adoption of ISO 27001 as a security control framework offers several benefits for executive management and the groups and individuals responsible for risk, security, compliance, and audit. The inherent benefits include:

- **A unified set of controls:** Organizations can centralize, manage, and satisfy multiple regulatory and compliance requirements through a single, unified set of controls.
- **Simplified production of audit evidence:** Evidence and metrics supporting the operational effectiveness of the controls can be reused, simplifying and reducing efforts required by external auditors and assessors for regulatory and compliance requirements such as Sarbanes-Oxley, SAS 70s, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) mandates, and Gramm-Leach-Bliley Act (GLBA).
- **Performance improvements:** Processes supporting the control objectives are assessed, refined, and improved, resulting in continued performance improvement of the security program.

## A Unified Set of Controls

ISO 27001 and ISO 27002 naturally map and align with other standards and compliance frameworks. For organizations dealing with Sarbanes-Oxley, IT general controls, and SAS 70s, ISO 27001 naturally maps into the security- and risk-related portions of the Control Objectives for Information and related Technology (COBIT) framework. For other compliance requirements such as GLBA, HIPAA, and PCI, ISO 27001 provides a superset of controls that covers and encompasses all of the security and risk-related controls.

When implementing a single ISMS with the intent of covering multiple compliance requirements, an organization first identifies the scope of the compliance requirements as they pertain to its assets, business operations, facilities, and IT processes. This drives the development of the necessary process flows. The process flows can then be aggregated into a single set or union of processes that fall under all of the compliance requirements.

The organization also must identify the mappings between the various compliance requirements to the ISO 27001 controls. These mappings should include the specific control requirements for each compliance initiative, which helps ensure that all requirements are addressed.

*While it may not be necessary to collect detailed metrics for every control, certain controls should naturally stand out as more critical either because of the risk they mitigate or the business process they support.*

As the organization performs its risk assessments on the processes, the organization will evaluate and classify, according to ISO 27001, the existing controls in place. It will also evaluate the applicability of the other ISO 27001 controls, taking into account the mappings to the other external compliance requirements. Some exposures may be unacceptable to management and will require risk mitigation or risk treatment plans before or in conjunction with the selection of controls.

As the organization selects the controls, it will likely also select other properties of the control. These include selecting the method of implementation or the process necessary to support the objectives of the control, the metrics that will be collected to determine the effectiveness of the control, the testing and validation procedures, and the frequency of the testing at the control level (as opposed to the auditing performed as part of validation of the entire ISMS).

## **Simplified Production of Audit Evidence**

As an organization works through the process of implementing an ISMS and selecting its set of controls, it must decide what types of metrics are important and for which controls. While it may not be necessary to collect detailed metrics for every control, certain controls should naturally stand out as more critical either because of the risk they mitigate or the business process they support. Other controls should be easily identified because of their natural links to external reporting requirements.

It is up to the organization to identify the type of information or metrics that would represent to themselves and management whether a control is operating effectively. However, since most organizations have at least one type of external compliance requirement, this should give them a start.

Organizations that have no external requirements can look to external sources that contain examples of metrics, such as NIST SP800-55, *Security Metrics Guide for Information Technology Systems*.

Organizations with multiple compliance requirements should be able to produce a single list that contains a ‘normalized’ set of required audit evidence for all requirements. This list should identify the format, structure, and contents of the evidence, as well as reporting frequency and retention requirements. By mapping these auditing requirements to their associated controls, an organization can use an ‘implement once, reuse many’ strategy for auditing. A possible beneficial side effect of working through this mapping is that organizations may also determine that, in certain instances, they are collecting and retaining evidence or documentation that is not necessary and can be eliminated.

Once implemented, the controls selected by the organization will produce the metrics and evidence supporting the effectiveness of the control. In addition, the owners of the control will be responsible for validating the effectiveness of the control by reviewing the metrics and performing the validation procedures according to the frequency and processes specified when the controls were selected.

*A properly implemented ISMS gives external auditors everything they need with respect to the validation of security controls. They will be able to re-validate that there is a formal risk assessment process in place and that the risk assessment process determined the appropriate control that mitigated the perceived risk.*

A properly implemented ISMS gives external auditors everything they need with respect to the validation of security controls. They will be able to re-validate that there is a formal risk assessment process in place and that the risk assessment process determined the appropriate control that mitigated the perceived risk. They will also be able to validate that the controls are operating effectively by reviewing the internal validation process and the metrics being generated by the control. This demonstrable evidence alone should significantly reduce the amount of effort required by the auditors for independent reviews and validation for areas covered by Sarbanes-Oxley, PCI, SAS70s, HIPAA, etc. For organizations wishing to have their ISMSs certified, this should further reduce the amount of effort required, since a third party is already auditing and validating the controls.

## Performance Improvement

When organizations proceed to implement each control, they can use what is known as the Plan-Do-Check-Act (PDCA) process. From a maturity standpoint, the entire PDCA process for each control will be documented and repeatable. The determination process during the planning phase includes more than just the identification of the appropriate process, procedure, or solution that supports a control. The organization will also decide the types of success criteria or key goal indicators ('outcome measures,' in COBIT terminology) that will determine whether the process is meeting the needs of the control objective.

In addition, the organization identifies the metrics that can be obtained from critical elements or steps within the sub-processes to show how well it is operating or performing. Collection and analysis of these key performance indicators by the control owners during the 'Check' phase can be used to identify where improvements or adjustments may need to be made (during the 'Act' phase) to satisfy the intent of the control.

On the other hand, if the process is operating effectively based on the performance indicators but still not meeting the intended goal or objective of the control, the cyclical nature of the PDCA process allows the organization to perform a root cause analysis, identify the cause(s), and make the adjustments necessary to the control's process. This continuous re-evaluation helps to improve the processes and their performance over time and ultimately improves the effectiveness of the security program.

## Conclusion

Whereas most organizations address their compliance requirements individually in a 'stovepipe' fashion, identifying the mappings between ISO 27001 and the other compliance requirements, an organization can implement a single security control framework in a manner that will satisfy all compliance requirements. Once in place, this single framework can simplify auditing and reporting requirements, reduce the amount of documentation to manage and records to retain, and facilitate demonstrable process and performance improvements.

*For more information about  
CTG's Security Services,  
please contact:*

Rob Keranen  
Senior Account Executive  
800 Delaware Ave.  
Buffalo, NY 14209  
541/550-8824  
[rob.keranen@ctg.com](mailto:rob.keranen@ctg.com)

*Backed by over 40 years' experience, CTG provides IT solutions and services to help our clients use technology as a competitive advantage to excel in their markets. CTG combines in-depth understanding of our clients' businesses with a full range of integrated offerings, best practices, and proprietary methodologies supported by an ISO 9001:2000-certified management system. Our IT professionals based in an international network of offices in North America and Europe have a proven track record of delivering high-value, industry-specific solutions. CTG serves companies in several industries and is a leading provider of IT and business consulting solutions to the healthcare market.*

*More information about CTG is available on the Web at [www.ctg.com](http://www.ctg.com).*

**A SPECIAL CLIENT REPORT**

---

*Confidential Information: Special Report and Analysis for CTG Client Use Only*