



White Paper

metagroup.com



800-945-META [6382]

January 2005

Unraveling Security and Risk Regulation

A META Group White Paper

“An organization’s success will be predicated on successfully implementing an effective risk management program, but its success will be measured by its interpretation and addressing of applicable regulation.”



METAGROUP

Contents

Introduction	2
<i>Where Did This Sudden Emphasis on Regulation Come From?</i>	2
Regulatory Requirements	3
<i>Accountability</i>	3
<i>Transparency</i>	4
<i>Measurability</i>	4
Addressing Regulation	4
<i>The Secret to Addressing Regulation</i>	4
<i>The Hierarchy of Controls</i>	5
<i>The Control Environment</i>	6
<i>Selecting and Defending Controls</i>	6
Achieving Compliance	7
<i>Continuous Compliance</i>	7
Bottom Line	8

Introduction

Regulation will remain the greatest driver for the implementation of information security and risk controls through 2010. An organization's success will be predicated on successfully implementing an effective risk management program, but its success will be *measured* by its interpretation and addressing of applicable regulation.

Where Did This Sudden Emphasis on Regulation Come From?

Risk management is about controlling risk to predefined and acceptable levels, which is something all organizations should be doing. The problem is, they haven't been. In fact, traditionally most information security risks have been written off as a cost of doing business.

Even before 9/11, the US government was working on cybersecurity through an effort to protect critical infrastructures in the mid to late 1990s, after recognizing the nation's growing dependence on computers and the Internet. Yet business was slow to respond. This was in small part due to conscious business decisions, but for the most part, businesses were ignorant regarding their dependence and the true level of the threat. In a post-9/11 world, this dependence and risk can no longer be ignored.

Other major factors regarding this increased focus on regulations include concerns related to privacy and corporate governance. Privacy was a major regulatory influence before critical infrastructure. Two of the most significant US regulations — the Gramm-Leach-Bliley Act (GLBA) and the Health Information Privacy and Accountability Act (HIPAA) — were enacted in the late 1990s with an emphasis on the privacy of personal data, with information security in a supporting role. Following various accounting debacles (Enron, WorldComm, Parmalat, etc.), it was clear that corporate governance and responsibility needed a boost. How can accountability, integrity, and privacy exist without security?

In 1992, US Representative Mac Thornberry (Republican — Texas), chairman of the House Subcommittee on Cybersecurity, Science, Research & Development said, "You don't want to be too quick on the draw with new mandates, but you can't be too hesitant to pull the trigger when there are concerns." Figure 1 provides a list of relevant cybersecurity regulations that many organizations currently face.

Figure 1 — Relevant Cybersecurity Regulations

Regulation	Who It Affects	Requirements
Sarbanes-Oxley Act (SOX)	All public companies traded on US exchanges	Controls to protect the integrity of financial reporting
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare providers and insurers, including self-insured companies	Separate requirement lists (rules) for the security and privacy of individually identifiable health information
Gramm-Leach-Bliley Act (GLBA)	Financial vertical	Security and privacy requirements for financial data
Federal Information Security Management Act (FISMA)	Federal agencies	Security controls, vulnerability assessment, and annual reporting
California's SB 1386 (Database Security Breach Notification Act) — similar laws in other states; federal bill pending	Companies that store personal data on California residents	Notification of individuals when the company reasonably believes personal data has been stolen

Source: META Group

Regulatory Requirements

Regulation must be addressed holistically, rather than with a piecemeal approach. To accomplish this, it is critical to understand the fundamentals of regulatory requirements, so a comprehensive, proactive program can be put in place that addresses all applicable regulations. All regulation requires and supports three basic tenants: accountability, transparency, and measurability.

Accountability

Accountability is required to know who did what and when, but it also requires clearly defined responsibilities. When many of the accounting debacles of the early 2000s occurred, there was a great deal of finger-pointing and little acceptance of responsibility. Accountability requires firmly placing responsibility with the individuals who have the power to control the risk.

Transparency

Transparency is visibility into the risk management controls, the business, and the assets being protected. Something cannot be protected if it is not understood. This implies the need for asset inventories, understandable security technology, and process formalization.

Measurability

Metrics enable measurement of the levels of risk. Regulators recognize that organizations cannot reduce risk to zero, so there will always be a level of residual risk accepted. Success (including compliance) requires mitigating an appropriate amount of existing risk, resulting in acceptable levels of residual risk. None of this is possible without effective measurement of risk posture levels.

Addressing Regulation

Most regulation is harsh and fuzzy. This is a bad combination for organizations struggling to address regulatory concerns. The laws themselves offer little insight into the actual requirements for the organization. For example, even the most detailed security laws will not indicate direct requirements for some the most common security mechanisms, such as intrusion detection, antivirus, and even firewalls. Frequently, clear control requirements are also missing from other sources (e.g., official guidance, audit standards, case law).

Frustrating as it may be, this lack of specificity is necessary. Laws must apply universally across different organizations and stand the test of time. Practically speaking, this means they must be flexible enough to work for organizations of different sizes, with varying complexities and threat postures. These laws must also accommodate advances in technology and the standard of due care. In short, a completely prescriptive regulation would apply to a very narrow set of organizations and be out-of-date before the ink was dry on the signature signing it into law.

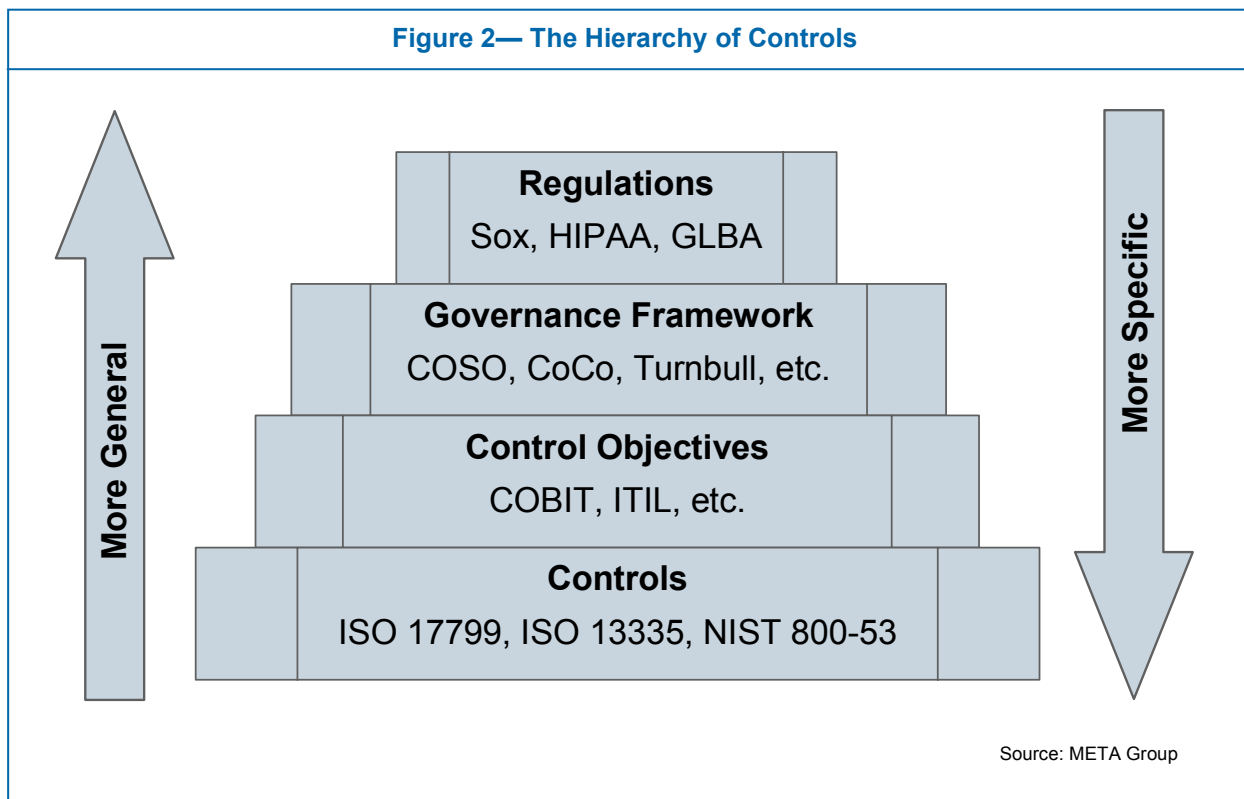
The Secret to Addressing Regulation

One of the significant ramifications of this lack of specificity is that organizations are challenged to know exactly what they should do and what equals compliance. The secret is that there is no definitive assertion regarding what equals compliance, so organizations are on their own to determine what is reasonable and appropriate for their organization. Lacking this definitive assertion, compliance becomes a negotiation with the auditor, and organizations must build a defensible case that their decisions are correct for their organization.

The Hierarchy of Controls

To resolve the issue of lack of regulatory specificity, we refer to a “hierarchy of controls,” which gives us a road map for implementation where guidance is unavailable (see Figure 2). This hierarchy starts with the specific laws at the top and then a corporate governance framework that sets high-level requirements to secure and control an environment. Each country has its own preferred national standard¹. In the US, the preferred framework is COSO², which identifies five inter-related components of effective internal control:

- The control environment
- Risk assessment
- Control activities
- Information and communications
- Monitoring



¹ For example, CoCo (Criteria of Control) reports, Turnbull Report, King Report, KonTraG, or other country-specific control frameworks

² The Committee of Sponsoring Organizations (COSO) Report, Internal Control - Integrated Framework

Below the governance framework in the hierarchy are the high-level control objectives established by control frameworks such as COBIT³ and ITIL⁴. These frameworks also provide guidance regarding the more specific control objectives and the processes required to achieve compliance. The bottom of the hierarchy is defined by specific security controls found in standards such as ISO 17799, ISO 13335, and NIST 800-53.

The Control Environment

The control environment is a basic set of principles that should reflect process, formalization, measurability, and control. These themes should be present throughout the environment and as part of all implemented controls:

- Configuration and change management
- Separate development, test, and production environments
- Segregation of duties
- Identification and authentication
- Clearly defined roles and responsibilities
- Least privilege
- Monitor, measure, and report
- Good documentation

Once an effective control environment exists, an organization can overlay specific controls to mitigate risk to predefined levels. Selecting reasonable and appropriate controls is a challenge in and of itself.

Selecting and Defending Controls

To select the right controls, organizations must develop a defensible case for reasonable and appropriate controls that address reasonably anticipated risks. These controls must be organized into a well-documented, proactive, and process-oriented program. Put another way, controls that are likely to pass muster with auditors should have the characteristics of being organized, well documented, and well thought-out, and should also address real threats while balancing cost and benefit.

Organizations can work toward these goals by taking the following steps:

- Identifying reasonably anticipated risks using an ongoing risk assessment
- Identifying a reasonable and appropriate set of security controls
- Creating a defensible case to support decisions
- Developing a proactive process-oriented security program

³ Control Objectives for Information and related Technology (COBIT) by the IT Governance Institute

⁴ Information Technology Infrastructure Library (ITIL)

Judging how much security is enough has become one of the greatest challenges that organizations face. If a regulation requires auditing, how much auditing is enough? If a regulation requires encryption, how much encryption is enough? Many organizations have established requirements that have overshot the bounds of “reasonable and appropriate” based on what their peers are doing and what is possible, given the maturity of current security solutions.

When addressing regulatory risks, organizations should strike a balance between meeting the letter of a regulation (or its interpretation) and developing controls that truly address risk in the enterprise. Organizations that focus on meeting regulatory requirements tend to accomplish only that goal. For example, a control to address log monitoring in the enterprise can be created that will pass muster with the auditors, yet provide no real value in addressing risk.

Achieving Compliance

As stated earlier, there is no definitive assertion of compliance. An organization must focus on developing effective risk management controls for the benefit of the organization as its primary objective, and then map those controls back into specific regulations.

Selecting a set of controls does not equal compliance and must be considered along with the business process. The specific requirements for compliance with each regulation are unique to each regulation, so they must be addressed individually. Organizations should develop a security program and select controls that address risk management in their specific organization. They should also create a compliance road map that maps these controls specifically back into regulatory requirements.

Using HIPAA as an example, we recommend that organizations select controls independent of the rule and then map them back into each of the 60 line items. It is important that a defensible justification be created for each line item of the rule that explains why the mapped controls meet the requirement. Gaps should be identified and addressed appropriately. This list of justifications is created to support actual compliance, not the mere existence of the controls.

Continuous Compliance

Compliance must be treated as a continuous process for many reasons. Enterprises are dynamic, and when something changes, compliance must be reassessed against the change. The threat environment is constantly shifting, and controls must be adjusted to respond to the current threat. The standard of due

care should be expected to rise, recognizing that what was good enough last year may not be good enough for this year or the next. Probably most importantly, the majority of the regulations require regular reporting or annual assessment. If an organization finds itself in an enforcement action, it should be prepared to present its latest case for justification of compliance.

Bottom Line

Regulation is a great motivator. Organizations must assess their threats, select reasonable and appropriate controls, and build a defensible case that they are compliant. Failure to do so leaves the organization open to the threat of non-compliance, which may involve fines for the organization and possibly jail time for the responsible individuals.

Paul Proctor is a vice president with Security & Risk Strategies, a META Group advisory service. For additional information on this topic or other META Group offerings, contact info@metagroup.com.



About META Group

Return On IntelligenceSM

META Group is a leading provider of information technology research, advisory services, and strategic consulting. Delivering objective and actionable guidance, META Group's experienced analysts and consultants are trusted advisors to IT and business executives around the world. Our unique collaborative models and dedicated customer service help clients be more efficient, effective, and timely in their use of IT to achieve their business goals. Visit metagroup.com for more details on our high-value approach.

