www.iss.net

Compliance, Part 1

Concepts, Controls and Due Care

Table of Contents

SO WHAT IS COMPLIANCE REALLY?

According to the American Heritage dictionary[1], **"comply"** means to act in accordance with another's command. In other words, "compliance" means to **obey *someone's* rule or set of rules**. However, in the context of recent government regulations, compliance requires that companies submit themselves to government-imposed legislation. This curt dictionary definition leaves us wanting more, does it not?

ACCOUNTABILITY, TRANSPARENCY AND MEASURABILITY

Myriad regulations pose a challenge to businesses, but commonalities exist among them all.

> *"All regulation requires and supports three basic tenets: accountability, transparency and measurability . . . Accountability requires firmly placing responsibility with individuals who have the power to control the risk. Transparency is visibility into the risk management controls, the business and the assets being protected. Something cannot be protected if it is not understood. Metrics provide for measuring levels of risk . . . Success means mitigating sufficient risk and leaving acceptable levels of residual risk.[2]"*

In other words, **Accountability** refers to holding specific persons responsible for the assets *under their ownership* to preempt any potential ambiguity associated with finger-pointing later.

Transparency refers to internal visibility (for the internal audit/compliance group), upper-management visibility, external visibility (namely, for the external auditors) and a more in-depth understanding of the affected business processes, assets and *controls* put in place to mitigate any reasonably anticipated risks posed against said assets.

Measurability refers to quantifying your risk exposure to prove that progress has been made toward reducing that exposure. This measurement of risk is inextricably tied to the assets themselves, as some assets are more critical than others. As well, measurability also refers to the documentation associated with selecting and justifying controls.

ETHICAL CONSIDERATIONS VERSUS LEGAL CONSIDERATIONS

Before various government regulations were imposed on public companies, the terms Accountability, Transparency and Measurability were primarily deemed *ethical* considerations. After the accounting debacles associated with Enron and WorldCom, however, the government took action to ensure that public companies would actively take steps to help rebuild investor and consumer trust in the security and legitimacy of corporate financial and personal data. New government regulations effectively *legalized* the terms, Accountability, Transparency and Measurability. Beyond ethical considerations, failure to meet certain standards of Accountability, Transparency and Measurability can result in jail time and/or hefty fines. In short, Accountability, Transparency and Measurability are no longer solely ethical issues but are now also required by law. Take the Sarbanes-Oxley Act (SOX), for example:

*"SOX's reqs [requirements] are intended to force management of public companies capitalized at $75 million or more to be **accountable and responsible** for their financial statements, the goal being to protect their investors from the perils of corporate collapse.[3]"*

*"One of the most important elements of SOX compliance is providing evidence that the financial applications and supporting systems and services are adequately secured to **ensure that financial reports can be trusted**.[4]"*

CONTROLS, CONTROLS, CONTROLS

The term 'control' appears quite often in compliance literature and its meaning has been clouded by overuse. Recall that government legislation was instituted to ensure that public companies would actively take steps to help rebuild investor and consumer trust in corporate financial and personal data.

*"Section 404 of the [Sarbanes-Oxley] Act **aims to strengthen the internal controls that underpin** the accuracy and reliability of a company's published financial information.[5]"*

The government intended (and now expects) companies to define processes and institute measures to ensure that data is protected from unauthorized disclosure and fraud. Think of these measures as controls. Or, more specifically:

"(a) control [is a] means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

NOTE: Control is also used as a synonym for safeguard or countermeasure.[6]"

However, it is important that we *do not* approach controls with a checklist mentality.

"The challenge is to focus on the most important things and not try to checklist everything. ***Wherever the most money and greatest potential for fraud exists, that's where auditors will investigate first****, and where IT architects need to focus their efforts.[7]"*

"Selecting a ***set of controls does not equal compliance*** *and must be considered along with the business process.[8]"*

Specific to Sarbanes-Oxley:

"[The Public Company Accounting and Oversight Board requires that companies] provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on financial statements.[9]"

In other words, for Sarbanes-Oxley compliance, in order to strengthen internal controls, companies must *take steps* to prevent or detect theft, unauthorized use, or asset transfer that could force restatement of company earnings. These steps are indeed the very *controls* required for demonstrating compliance. Consider the following examples of the different types of *controls*: physical, technical, administrative, business and process.

GUNS, GUARDS AND DOGS

Some familiar, traditional controls — guns, guards and dogs — are specific examples of **physical controls**.

How do physical controls address risk? Consider a burglar attempting a break-in. Deadbolt locks on the doors hinder easy entry, a security system would alert police and neighbors almost immediately, guard dogs posted outside and maybe even a firearm inside are additional deterrents.

A combination of controls alerts and protects homeowners from potential break-ins. Note also how using individual, complementary controls in combination provides greater security and assurance. For example, deadbolt locks on the doors may secure the doors but not the windows. The importance of combining multiple security controls cannot be understated.

WALLS OF FIRE AND SYSTEMS TO PREVENT INTRUSIONS

Another type of control is a technical or technology control. Physical controls like access cards and security guards can prevent unauthorized users from gaining access to the critical data available in the server room. But the computer and Internet age complicate matters. Technical controls such as intrusion prevention systems are required to prevent a 'remote compromise' of a server or system that can be initiated over the network connection from almost anywhere.

8 A.M. TO 6 P.M. ACCESS ONLY

To illustrate **administrative controls**, imagine that employees are only allowed access to company resources from 8 a.m. to 6 p.m. Documenting and distributing this policy is considered instituting an administrative control.

> *"Administrative controls are primarily policies and procedures to control the actions of people. Administrative controls can also embed technology such as enabling password aging (technical control) to enforce a policy of changing passwords every 60 days (administrative control). Examples of administrative controls are acceptable-use policy, media control policies, sanction policies and training.[10]"*

Additional physical and technical controls applied in conjunction with the 8 a.m. to 6 p.m. access rule strengthen the company's security posture. For example, building entry via access cards and network access via firewall rules could be restricted during off hours.

ORGANIZATIONAL RISK

Not all controls relate specifically to physical or information security. Compliance demands a broader view of risk management. Some examples of **business controls** include requiring at least two people to sign checks and running background checks on new hires.

A PROCESS FOR EVERYTHING

Process controls can arguably be considered a subset of administrative controls. They remain set apart because compliance calls for a process-oriented security program, making process controls particularly notable.

> *"Process controls are formalized procedures that are repeatable, survivable from one person to the next, and measurable. Process controls are manual . . . Examples of process controls are incident response, configuration management and vulnerability management.[11]"*

Part 2 of this white paper explains the importance of documenting security processes before the auditors, and illustrates how a comprehensive, centralized security management tool helps to define security process and supply documentation to support the process.

MESH OF CONTROLS

Coverage of the different types of controls is not comprehensive but rather illustrates that focusing on one type of control would be detrimental to the others, short-sighted and worth only partial credit, so to speak. In other words, using a combination, or mesh, of controls can actually strengthen your case before the auditor when it is time to justify, document and defend.

*". . . **[V]arious levels of controls can be adopted for any given risk**, depending on the business's attitude toward that risk and the prevailing standard of due care.[12]"*

*"View controls collectively — **using a mesh of controls that support each other can strengthen justification.**[13]"*

THE STANDARD OF DUE CARE

So far, the discussion of compliance has focused on properly addressing risk through controls. But what if a company decides to accept a particular level of risk because it can confidently build a case for not addressing that risk? After all, accepting a certain level of risk appears to be a valid option.

*"[O]ptions for risk treatment include: . . . knowingly and objectively **accepting risk**, providing [it] clearly satisf[ies] the organization's policy and criteria for risk acceptance.[14]"*

Faced with answering to the auditors, does compliance, at some point, shift from addressing risks to justifying decisions? Does the compliant state of the enterprise simply become a debate rather than a negotiation? This, of course, is not the case; however, it brings up an important point.

*"It is important to remember that various levels of controls can be adopted for any given risk, **depending on the business's attitude toward that risk and the prevailing standard of due care**.[15]"*

In other words, a business can choose to accept risk as long as no prevailing standard of due care exists. However, if a prevailing standard of due care does exist, this standard supersedes the business's evaluation of risk and demands that the risk be addressed even if the business initially chose not to.

STANDARD OF DUE CARE . . . IS IT JUST LEGALESE?

So what is this standard of due care anyway?

"The standard of 'due care' is that level of diligence which a prudent and competent person would exercise under a given set of circumstances. 'Due professional care' applies to an individual who professes to exercise a special skill such as information systems auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by practitioners of that specialty.[16]"

ANTIVIRUS EXAMPLE

For example, choosing to forego antivirus security would not be an acceptable level of risk because antivirus has become part of the standard of due care. This established standard of due care would prevent an auditor from signing off on compliance. So, even though compliance is primarily a negotiation with the auditors, there are certain minimum requirements *not* up for negotiation that will take precedence over the results of a company's individual risk assessment.

RISING STANDARDS

Just when a company believes it has met the standard, it realizes the target has been moving all along.

*"The **standard of due care should be expected to rise**; consequently, what was good enough last year may not be good enough this year or the next.[17]"*

Wait a minute! What is causing this standard to rise? Consider the previous antivirus example.

*"**Traditional signature-based antivirus product[s] can no longer protect companies** from malicious code attacks.[18]"*

Clearly, the decreasing security effectiveness of antivirus security leads to a higher standard of due care, which may call for more proactive security measures such as host-based Intrusion Prevention Systems.

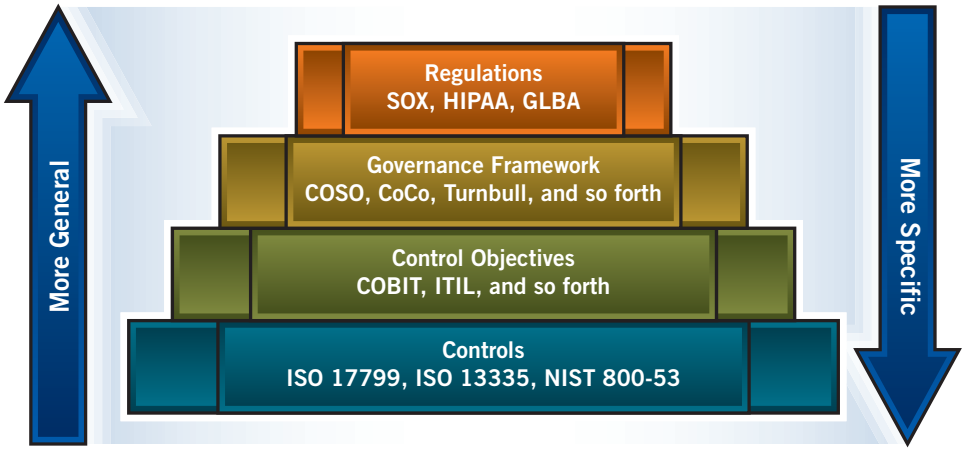
Part 2 of this whitepaper will address the benefits of proactive vulnerability protection as opposed to reactive threat countermeasures.

When considering the standard of due care, remember that there are now two factors to consider when conducting risk assessment and selecting controls:

- *Select reasonable and appropriate controls to address reasonably anticipated risk as discovered by internal risk assessments*
- *Be mindful of the prevailing standard of due care (as well as current events that could cause this standard to rise) which affects corporations regardless of the results of their own risk assessments.*

WHERE TO FIND GUIDANCE?

But which controls should be implemented, in what order, and how does a company know it's been comprehensive in addressing risk? Because regulations are ambiguous, organizations are not sure what they should do to demonstrate compliance. The hierarchy of controls (illustrated below) provides a way to map controls back to those ambiguous regulations. Though these frameworks and best practices are not required for compliance, they often provide clarity when no other guidance is available.



Source: Gartner (January 2006) [19] 136911-1

In fact, by leveraging these frameworks and best practices, companies will more than likely realize a business benefit in addition to meeting requirements for compliance. In fact, documenting this mapping can be useful as part of a defense and justification before the external auditor. This enables auditors to better understand the thought process, logic and justification for compliance-related decisions.

When referencing these frameworks, however, be sure to tie the requirement and associated controls back to a top-down, risk-based assessment. Otherwise, simply following a checklist mentality may not address the risk required by compliance.

*". . . **[J]ust because a control addresses a governance objective doesn't mean it will mitigate a reasonably anticipated risk** — and therefore it may not meet your needs for risk abatement or the auditor's expectations for regulatory compliance.[20]"*

*"The SEC [Securities and Exchange Commission] also criticized companies for taking a "mechanistic, check-the-box approach," rather than a **top-down risk-based assessment**.[21]"*

WHICH CONTROLS SHOULD BE IMPLEMENTED FIRST?

Every company has resource constraints and will inevitably question which controls it should select and implement first. Because each company's situation is different, the best guidance is also the most intuitive — focus on the greatest risks first.

*"The challenge is to **focus on the most important things** and not try to checklist everything. **Wherever the most money and greatest potential for fraud exist**, that's where auditors will investigate first, and **where IT architects need to focus their efforts**.[22]"*

THE GROWING ROLE OF INFORMATION SECURITY

Business controls such as two-person check signing reduce the chance of fraud and strengthen the compliance effort. However, the importance of information security should not be overlooked:

"Although management and business units are responsible for using personal information appropriately, ***it's up to security professionals to protect it****.[23]"*

*"****CIOs and IS are central to implementing internal controls*** *by providing controls in finance systems and applications.[24]"*

In fact, information security's history of security policy enforcement makes it uniquely qualified to address the auditing and enforcement issues surrounding regulatory compliance.

PROCESS ... HOW ARE COMPANIES TACKLING COMPLIANCE?

Several approaches are outlined below, but it is critical to emphasize that whatever approach is chosen must be *risk-based*.

"Preliminary research indicates that ***businesses that do not take a risk-oriented approach to Sarbanes-Oxley compliance will find themselves spending much more*** *on compliance efforts than necessary.[25]"*

Rather than checking off a list of controls, companies must look at how risk is impacting their environment and develop, document and justify their control selection based on those risks.

[One proposed process]

- *"Set up the compliance project, led by finance, with IS [Information Security] as a key team member.*
- *Identify the critical IS processes. Finance must define what is material to the enterprise, then IS can use this to decide which IS processes could affect financial reporting.*
- *Assess risks and design controls. Conduct a risk analysis for each of the critical IS processes to see where internal controls are needed. These controls are then designed and implemented.*
- *Test controls and document the results. Create a test plan and test internal controls. Identify, rectify and retest weak internal controls.*
- *Attest to results. Prepare and submit the correct documentation to the regulator.[26]"*

[Another process geared specifically toward security groups]

- *"Develop a security program and select controls that address risk management.*
- *Create a compliance road map that maps such controls specifically back to regulatory requirements.*
- *It is important that you create a defensible justification for each line item that explains why the mapped controls meet the requirement.*
- *Identify gaps and address them appropriately.*
- *This list of justifications should support compliance rather than supporting the mere existence of the controls.[27]"*

JUSTIFY, DOCUMENT, DEFEND

A discussion about compliance would not be complete without referencing the auditing community. Think of an auditor as an agent of the government who ensures that companies are meeting compliance requirements. The Public Company Accounting and Oversight Board (PCAOB) was created to provide auditors with additional guidance on conducting an audit. In May 2005, it issued additional guidance beyond Auditing Standard No. 2 to lend further insight into what auditors should be looking for in their audits.

"The overall objective of Auditing Standard No. 2 is for the auditor to ***obtain evidence that a company's control system reasonably assures that its financial statements do not contain material misstatements.***[28]*"*

"External auditors need to conclude two things:

- *"They must be convinced that controls are working and are adequate.*
- *"They must be convinced that management's evaluation of controls was reasonable and adequate.*[29]*"*

Because no one set of compliance requirements applies across the board, it is important to realize that a company's state of compliance is contingent upon negotiations with its auditor.

*"****Compliance isn't an absolute state but a negotiation*** *between your company and its auditor. Therefore, you must* ***create a defensible position*** *with respect to Sarbanes-Oxley Section 404 compliance, because* ***a definitive one is not possible****.*[30]*"*

*"****Ultimately the decision that an organization is in compliance rests with the auditor*** *or regulatory body assigned to test and verify controls. Organizations must prepare to* ***defend their decision and make a strong case that they made the right decisions*** *for their organizations.*[31]*"*

It is therefore necessary to document the risk assessment, the selection of controls and testing, then proceed to justify and defend why your decisions were the right ones for your organization.

"A ***documented control process*** *that will mature with time is a strong foundation to build a defensible case for compliance.*[32]*"*

"You must justify and document all decisions. Justifications should include the output of ***risk assessment and controls selection criteria****. View controls collectively — using a* ***mesh of controls*** *that support each other can strengthen justification. Neutral,* ***third-party evaluation*** *will add credibility to the process . . . Showing a* ***track record of improvement*** *also will allow you to better defend your company's controls.*[33]*"*

In summary:

"Compliance means that you must ***document and demonstrate that material processes are documented and sufficient controls*** *are in place and that they are regularly tested. You must have an argument to* ***justify every decision****.[34]"*

RISK ABATEMENT, STRENGTHENING JUSTIFICATION AND DOCUMENTING THE SECURITY PROCESS

Part 2 of this white paper goes into greater depth on the topics of proactive risk management and abatement, the benefits of a centrally managed "mesh" of technical security controls and documenting the security process. It can be found at http://www.iss.net/support/documentation/whitepapers/index.html.

ABOUT INTERNET SECURITY SYSTEMS, INC.

Internet Security Systems is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. ISS products and services are based on the proactive security intelligence conducted by ISS X-Force® research and development team — the unequivocal world authority in vulnerability and threat research. With headquarters in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 800-776-2362.

BIBLIOGRAPHY – PART I

[1] The American Heritage Dictionary of the English Language, Fourth Edition, 2000

[2] Gartner, "The Chief Information Security Officer's Guide to Compliance," 12 January 2006, ID Number: G00136911

[3] IT Architect, "Crushing Compliance," 12.05, Vol. 20, No. 12, p. 32

[4] Information Security Magazine, "SOX Security School," http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1169201,00.html

[5] PCAOB Release No. 2005-009, May 16, 2005, http://www.pcaobus.org/Rules/Docket_008/2005-05-16_Release_2005-009.pdf

[6] ISO 17799:2005 (available for purchase at http://www.iso.org/iso/en/ISOOnline.frontpage)

[7] IT Architect, "Crushing Compliance."

[8] Gartner, "The Chief Information Security Officer's Guide to Compliance."

[9] PCAOB Auditing Standard No. 2, http://www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.2.aspx

[10] Gartner, "See Information Security Through the Controls and Policy Lens," 24 January 2006, ID Number: G00136810

[11] ibid.

[12] ibid.

[13] Gartner, "Select and Implement Appropriate Controls for Regulatory Compliance," 16 November 2006, ID Number: G00131086

[14] Gartner, "Maintain Regulatory Compliance Without Neglecting Security," 22 February 2005, ID Number: G00126117

[15] Gartner, "See Information Security Through the Controls and Policy Lens."

[16] Information Systems Audit and Control Association, "IS Auditing Guideline, Due Professional Care", 1999, Document G7

[17] Gartner, "The Chief Information Security Officer's Guide to Compliance."

[18] Gartner, "Magic Quadrant for Enterprise Antivirus, January 2005: Vendors Must Address New Malicious Code Threats," February 22, 2005, ID Number: G00125531

[19] Gartner, "The Chief Information Security Officer's Guide to Compliance."

[20] Gartner, "Findings From the 'Compliance and Risk' Research Community: Look For The Intersections Between Risk Assessment and Control Objectives," 10 January 2006, ID Number: G00137299

[21] IT Architect, "Crushing Compliance."

[22] ibid.

[23] Gartner, "Maintain Regulatory Compliance Without Neglecting Security."

[24] Gartner, "Sarbanes-Oxley: An External Look at Internal Controls," August 2004

[25] Gartner, "Findings From the 'Compliance and Risk' Research Community: Compliance is Driving Interest in Risk Management," 11 January 2006, ID Number G00137184

[26] Gartner, "Sarbanes-Oxley: An External Look at Internal Controls."

[27] Gartner, "Select and Implement Appropriate Controls for Regulatory Compliance."

[28] PCAOB Release No. 2005-009.

[29] Scott Landes, Manager of Financial Controls, Internet Security Systems (ISS), in conversation.

[30] Gartner, "Implement Security Controls to Comply With Section 404 of Sarbanes-Oxley Act," 7 October 2005, ID Number: G00127941

[31] Gartner, "The Chief Information Security Officer's Guide to Compliance."

[32] IT Architect, "Crushing Compliance."

[33] Gartner, "Select and Implement Appropriate Controls for Regulatory Compliance."

[34] Scott Landes, ISS, in conversation.