Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Institutional Need for Comprehensive Auditing Strategies

This paper examines the challenges in today's regulatory environment for financial institutions (primarily from the large institution's perspective, since they undergo the greatest scrutiny) and makes the argument that a high level, comprehensive auditing strategy is needed to allow organizations to respond effectively. In recent years, operational risk, as it relates to information security, has become more and more the focus of regulatory agencies and standards groups (e.g., NAIC, Basel II, BITS, FFIEC and many other...

Copyright SANS Institute
Author Retains Full Rights

AD
CloudLock
What's your cloud data security score?
L H
Google Apps
salesforce
Find Out

GIAC Security Essentials, version 1.4b

The Institutional Need for Comprehensive Auditing Strategies

By Stu Milus

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Institutional Need for Comprehensive Auditing Strategies

Abstract

This paper examines the challenges in today's regulatory environment for financial institutions (primarily from the large institution's perspective, since they undergo the greatest scrutiny) and makes the argument that a high level, comprehensive auditing strategy is needed to allow organizations to respond effectively.

In recent years, operational risk, as it relates to information security, has become more and more the focus of regulatory agencies and standards groups (e.g., NAIC, Basel II, BITS, FFIEC and many others). Why is this happening? Assessing business risk has been around along as business itself, but the present migration to e-Business and it's related exposures has caused business and its related regulatory agencies to examine the need and set expectations for appropriate risk preparedness. But establishing these expectations – also known as industry good practice - is only Part I of the work that needs to be done. Readying an organization to respond is Part II.

This paper begins with a definition of auditing, as the word "audit" can mean different things to different people, and contrasts the use of auditing in data processing's early days to its function in the world of IT, today. The intent is to show that the interconnectedness brought about by business conducted over the Internet alters the scope and approach of audits. Audits once performed at the application or line of business level, though still necessary, are no longer sufficient to surface and assess all exposures created by the new environment. Further arguments elaborate on the impact and implications of the technology that have enabled e-Business and show not only the distinctions between past and present environments, but also become a requirements list for a comprehensive audit strategy. Finally, a series of recommendations are made that outline the foundational elements an organization needs to enable an effective strategy.

Auditing in IT

As long as there's been a prescribed method for doing things there's been a need to audit. First, to see that the methods are being practiced and, second, that they're being practiced correctly. As defined by the ISO standards body, the audit function allows us to, "…carry out periodic reviews of security risks and implemented controls to take account of changes to business requirements and priorities, consider new threats and vulnerabilities, and confirm that controls remain effective and appropriate" (ISO/IEC, p. ix). Auditing is an after-the-fact detailed review of a system, and, in the world of Information Security, is considered a line of defense. It doesn't stop intrusion, but by requiring a logical explanation of what is seen, it helps identify when and where it happens (SANS Security Essentials 1.5 p. 6-8).

Information systems, by their very nature, are processes that support a variety business, government, or service needs. And, as such, are replete with "good" or required practices established by standards organizations. Early data processing mostly reflected systems written to take over routine accounting or

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

inventory management functions. The standards that existed in support of the manual activity could be adapted to support its automated version. Since, in most cases, the manual process had been around for a long time, it was likely the related audit process had, as well. All of the know-how of audit execution and remediation gained from long experience with the manual process could be applied to the automated one.

But as the field of computer technology developed it became an enabler of function and service; function and service that could not have existed or developed independent of it. Even the evolution of the name from Data Processing to Information Technology indicates a lot has changed. True, the sophistication of computer tools has continued to increase: spreadsheets, CAD systems, desk top databases, word processors, to name a few, are tools that business today would be hard pressed to do without. Yet, these tools are still pretty much just a faster, sometimes more accurate, means of doing what humans had done before with "pencil and paper." Even the gleaning and culling of data in such things, as decision support systems, though innovative, are simply a faster way of executing a model previously executed manually.

So, what are these things now enabled by technology that could not be classed as mere automated replacements for manual systems? Is there anything a computer can do that a human or group of humans, given ample time and know how, could not do?

The issue is not necessarily the computerized tools used, but rather the breadth of their implementation. We now have whole sets of business transactions that occur, start to finish, without human involvement on one or both sides of a transaction. Not only that, but they can occur without respect for geological or political boundaries. And, most importantly, access to this type of technical ability is available to anyone with a computer that can run an Internet "browser" application. The US General Accounting Office's (GAO) report on Critical Infrastructure Protection of February 28, 2003 states:

> Since the early 1990's, an explosion in computer interconnectivity, most notably growth in the use of the Internet, has revolutionized the way that our government, our nation, and much of the world conduct business. The benefits have been enormous. Vast amounts of information are now at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups (Tauzin/Dingel, p.1).

So again, it's not the level of computer tool sophistication, but rather, the fact that sets of these tools can be linked or networked together that is significant. As authors Carl Shapiro and Hal Varian put it, "…the new information economy is driven by the economics of networks." It's not just the information, but the supporting structure that enables search ability, availability, and connectivity that greatly increases "the value of the underlying information itself."

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This connection or network of computers fosters an environment that supports a type of commerce, communication, and entertainment that could not exist without it. Of course shopping from home via catalog or phone, video or teleconferencing, and special entertainment (Pay-per-view, for example) exist apart from the Internet and may continue to fill nitch-markets indefinitely. But the strength of the Internet lies in its reach and the fact that it lets users interact more directly with other users. The location independence and the real-time transactions have created opportunities pre-existing systems could not hope to provide.

Auditing e-Business: The Auditing Approach Will Have to Adapt to the New Environment

Use of the Internet is not just another way of doing business. It's not a simple replacement for the telephone or mail system. It's more akin to the revolution brought about by the automobile. As automobiles proliferated they brought about vast changes in government, law, commerce, how people thought about where they lived and worked, and much more (Ellul, p70). The Internet has affected each of those elements considerably and it's only in its infancy. More to the point, though it's opened a good deal of opportunity it has brought with it the challenge of managing this vast new environment.

Also, the breadth of risk is huge. With the continued migration to e-Business, more and more critical aspects of business rely on the security and availability of the Internet. However, due to the relative newness of the environment, business is still coming up to speed on both its use and pitfalls. Doing business over the Internet has become one more element to add to the list of the risks in doing business. However, due to the things shared in the preceding section, heightened awareness of the need for a more holistic view of an institution's operational risk is surfacing. And, as it's surfacing, we're finding the associated risks as expansive as the opportunity. The Zeichner Risk Analytics group says it like this:

> The importance of cyber-security protection has grown significantly in the past several years, especially with regard to national economic assets and the public's health and welfare. The tools of cyber disruption are widely disseminated. A single, knowledgeable terrorist or malicious hacker can disrupt state and local services at great speeds (Zeichner/Almosd, page 3).

And, if anyone should think that the concern over cyber-security is over blown, consider the following statistics. According to a report published by Internet Security Systems, Inc. (ISS), between the 4th quarter of 2002 and the 1st quarter of 2003, computer security incidents and detected attacks against businesses worldwide increased 37%. The same report estimated that there are now upwards of three million people in the US alone perpetrating cyber-attacks. ISS does not believe all three million to be hard-core hackers, "a lot of them are just taking tools that are out there, putting them together and seeing if they work" (Niccolai, p.3). Nonetheless, it is malicious behavior and cause for concern.

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ISS's findings are further supported by a survey conducted by Icsa Labs, a division of TruSecure, who not only found the frequency of incidents increasing (see Figure 1), but the costs to recover from an attack are rising, as well. For firms of 500 PCs or more, the average cost to recover from a virus increased by 15%, or 20 to 23 person days, from 2001 to 2002 (Bennett).

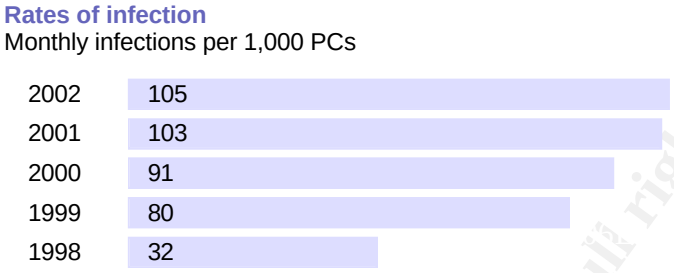


Figure 1

Finally, GAO's February report sited above says, "The risks associated with our nation's reliance on interconnected computer systems are substantial and varied." According to surveys conducted in 2002 by the FBI and the Computer Security Institute, 90% of respondents – mostly large corporations and governmental agencies – had detected cyber-security breaches. The GAO report goes on to say that incidents reported to Carnegie-Mellon's CERT® Coordination Center have climbed from 9,859 in 1999 to 82,094 in 2002. The worst is, CERT® estimates as many as 80% of security incidents go unreported. (Tauzin/Dingel, p. 7-9).

The Internet is already vast and it's still growing. A number of the threats and vulnerabilities have been identified with sound controls defined; however it's also understood that we don't know them all. And because we know the risk is real a lot of attention is being given to assessing and preparing for that risk. A business that chooses to do business over the Internet is stepping into a world largely uncharted.

So again, the new world of computer interconnectedness requires organizations take a second look at not only the security controls they must put in place – which are many – but also the process for overall review of if and how those controls are implemented.

Auditing Considerations and Requirements

Integration between once disparate parts of an organization are now enabled and required when business is transacted over the Internet. In the following section, exposures created in these new relationships, elements that would need to be considered in a comprehensive auditing strategy, are discussed.

Breadth of Risk:

As stated above, the purpose of an audit is to carry out periodic reviews of security risks and implemented controls. But as this paper has so far inferred, the

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

number of exposures are considerable. For example, The ISO/IEC[1] 17799 security standard is eleven categories and 65 pages. The Information Security Forum's (ISF) Risk Management Matrix, a standard of good security practices, is eighteen categories and 129 pages long. These standards of good practice outline controls for not only watch dogging networks and password strength, but also physical security and recommendations on the handling and hiring of personnel. It's also important to note that an organization that chooses to adopt one of these standards cannot pick and choose between what controls they'd like to employ, but must tend to all categories and implement controls for each.

Additionally, new combinations of exposures exist. First, the best information security controls are of no value if physical controls are lacking. What was put into place to guard the virtual environment can be easily traversed if someone wanting to get into your network can simply walk into your place of business and log on to a trusted device. Secondly, response to physical thefts, once relegated to recovering the stolen property, now have to add process for determining the information exposure if the items stolen were electronic information devices.

Old Boundaries Are No Longer Boundaries

In her book, "In Praise of Good Business," Judith Bardwick talks about the new "borderless economy." At one time, businesses could afford to ignore certain would-be competitors because of insulating geological and/or political boundaries. Not any more. As the Internet has created whole new sets of customers, once removed because of these old boundaries, it has also introduced whole new sets of competitors. Also introduced are new sets of people waiting to take advantage of an un-policed environment. The walk-in, drive-in, dial-in, click-in world intended to create conveniences for customers and efficiencies for business does the same for thieves.

The fact that information is considered an asset is not new; however, the virtual assets of a few years ago could be protected much the same way the physical assets had been. Computer systems could be located in secure areas, system access was relegated to members of the organization, and transmitted data was sent via private networks. In other words, the exposures were more finite and controllable. However, as innovation marches toward constant connection and anywhere-access, old perimeter protection techniques fail. Mobile computing pushed the perimeter beyond all conventional physical boundaries, as the perimeter extended to the most remote computing device. And, with the advent of wireless technology, the border between public and private access no longer exists.

Technological – Everybody's Got a Super Computer

As reported above, the number of malicious cyber-activities is increasing. This is due to the fact that the technology readily available to anyone that can turn on a computer is quite sophisticated. Hacker sites contain password cracking

[1] International Organization for Standardization/ International Electrotechnical Commission

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

software as well as scanning tools and denial-of-service programs. Not only that, but the sheer size and strength (memory and speed) of inexpensive, if not free, computers is enough to enable real time brute force attacks for all would-be hackers.

New relationships: Outsourced IT

As business has embraced the world of computer automation, how to accomplish the programming needs has morphed from in-house data processing departments to a variety of alternatives:

1) Outsourcing part or all of application development
2) Outsourcing support of existing applications
3) Purchasing services hosted at a service provider's site.

All of these options, and their permutations, create a whole new body of exposures. Not only does an organization have to create and enforce policies to secure its own environment, it now has to extend its arm of inspection to its service providers. After all, regardless of the soundness of the organization's security, the controls employed become virtually ineffective if its service providers, who supply code and have ready access to the its network, are laden with exposures.

If that were not enough, this scenario is further complicated when these functions are performed "offshore." Now distance, time zone, international law and political climate are added to the list of concerns.

Increased Regulatory Focus

As more critical business functions are enveloped in the e-Business environment, risks extend beyond the business itself to its customers and other businesses. To stabilize the economy and business environment, a great deal of regulatory interest has been raised. For example, California enacted privacy law CA Civil Code 1798.82, .84 (SB 1386) in September of 2002. Basically, any business that owns computerized data containing personal information must be ready to notify any California resident should it discover or be notified of any breach in the security of the data system (Huber/Cook, p.10). The Basel Capital Accord (Basel II) intends to establish a means to assess a bank's operational risk and levy reserve requirements accordingly. As well, banks will be expected to disclose information about the process used to manage and control operational risks.

These are but two examples of legislative oversight being focused on business transacted over the Internet or transacted by a business with Internet exposure. A few others are (Zeichner/Almosd):

1. Office of Thrift Supervision (OTS)
2. Office of the Comptroller of the Currency (OCC)
3. Graham Leach Bliley Act (GLBA).
4. Federal Deposit Insurance Corporation (FDIC)
5. Securities and Exchange Commission (SEC)
6. Federal Financial Institutions Council (FFIEC)

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7. HIPPA

Though not an exhaustive list, it does highlight the realization of government and industry that threats to cyber-space infrastructure are real and many. The Zeichner Risk Analytics group says it this way:

> Federal government agencies are advancing well beyond security programs for protecting customer information. The Federal Financial Institutions Examination Council (FFIEC) recently released the first of ten booklets on information technology security and management - the *Information Security IT Examination Handbook*. This handbook, which updates the FFIEC's 1996 requirements, addresses not only safeguarding customer information, but also performing risk assessments, detecting and responding to intrusions, and defeating malicious code attacks through effective management practices (Zeichner/Almosd, p.6).

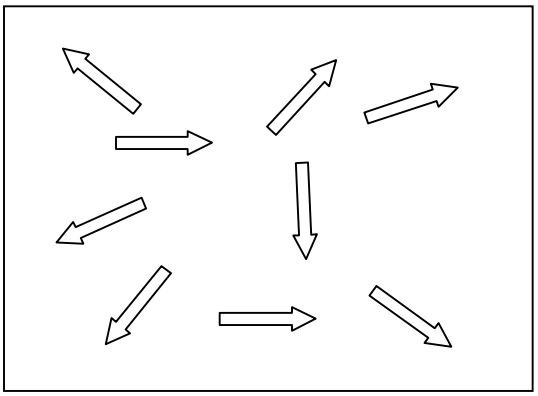
Organizational Structure

Organizational structure exists to support, among other things, lines of authority to identify and coordinate activity and function. It enables progress by establishing and maintaining order among the constituent parts of the organization. It's well understood that organizational structures have to adjust to their ever-changing environment if they are to remain effective; organizational resilience is necessary to remain vital and competitive. The continual migration to e-Business is forging new relationships within the business domain such that parts of the business, once totally unrelated, now share a need for integration. When once separate parts are now more closely related and, more importantly, governed, the challenge to reorder the lines of control is significant.

The purpose of a strategy is to establish vision or long-term goals such that all of an organization's resource can be aligned; tactical planning of all its constituent parts can focus on producing the same ends. As the strategy creates a planning focus it also brings with it a degree of extensibility. That is, an organization with a solid strategy is better positioned to respond the future unknowns because it has fewer internal corrections to make. When the landscape changes, the different parts, already moving in tandem, can respond with fewer internal conflicts.

For example, figures 2 and 3 show two organizations, one without a sound strategy and one with definitive direction. Imagine both organizations needing to respond to some change in their environment. For the purpose of this example, say the organizations needed all of their constituents to head south. For the organization in figure 3 it's a simple matter of asking its players to turn 90 degrees to their right, while the other organization must first identify the variety of current directions and then define appropriate instructions for each.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



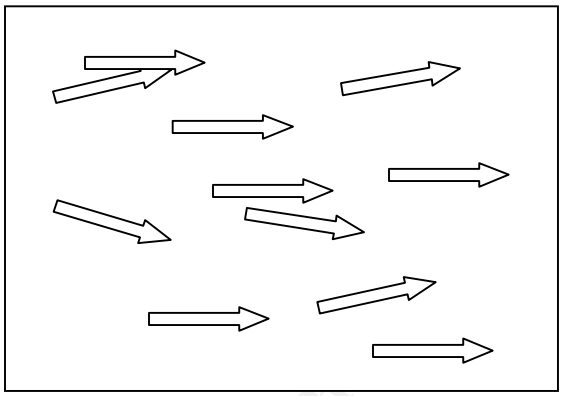


Figure 2: No strategy, no common direction Figure 3: Strategy creates common direction

In the world of e-Commerce it's likely the landscape will be shifting for some time as regulatory bodies continue to respond to the growth in this sector. As well, the environment is further complicated by state-to-state, national, and international jurisdictional differences. In short, organizations without a consistent and comprehensive means to assess their compliance with regulatory standards will find it hard to keep up with new legislative requirements.

Auditing Recommendations: Components of a Comprehensive Auditing Strategy

High Level Organizational Sponsorship

Earlier, the subject of organizational structure was discussed. At that point it was argued that the current chain of command could inhibit comprehensive auditing measures. By definition, a comprehensive auditing strategy means it's a strategy that applies to everyone. And while everyone may agree that working together would be more efficient cost effective, and generally a better way to go, it's likely the process would often stall out due to differences of opinion, philosophies, and interpretation of law, etc. In these cases, there has to be a tiebreaker; a single decision maker to keep the process on track.

Therefore, it's vital that the scope of authority behind execution of the strategy is high enough to encompass all parties involved. If the line of authority is aligned with the organization's existing reporting structure the implementation and execution of the strategy should find few barriers. For example, say the CEO is the strategy sponsor. Since the CEO has both the responsibility and authority to see that comprehensive audits are successful, expectations for appropriate attention and compliance cascade through the reporting hierarchy.

On the other hand, the sponsorship for the auditing strategy may not align well with the existing reporting structure. In that case, a "virtual authority" would have to be created to oversee the coordination of all auditing efforts. This could be something like an Auditing Office or an Audit Committee comprised of department representatives. Either way, the authoring authority still has to be

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

high enough in the reporting hierarchy to be the single decision point, when necessary.

Enterprise Information Security Policy

The next pivotal element is the establishment of an Information Security Policy that will apply to the entire enterprise. The policy becomes the "constitution" the enterprise uses to base future decisions and sets the bar for compliance. It's the element used to force compliance; the element that requires the organization to respond to audit findings and recommendations.

The policy gets its strength and authority from the fact that it:

1) Is backed by a high level sponsor, usually the president or CEO
2) Incorporates legislative requirements
3) Is constructed and ratified by representatives from throughout the organization - people don't argue with their own data

The construction of the policy should be based on an existing standard of good practice, such as the ISO 17799. This not only saves a great deal of time, but allows the organization to build on a foundation already recognized as sound. Standards groups, such as ISO, build their recommendations and requirements with a great deal of input from industry and government. Generally, compliance with such standards is viewed as acting with "due diligence."

A Single Body of Controls

At the center of a comprehensive audit strategy stands a controls framework; a single set of rules that multiple groups can build to and audit and assess against. Like the environment it supports, it is a living set of rules, standards, and guidelines that adapt to new technologies or newly discovered vulnerabilities. It is used to determine what is audited and to ensure all areas that need inspection are, in fact, inspected. In short, it serves to coordinate and integrate the many auditing activities.

As mentioned, the many new relationships of interconnected e-Business require a new perspective – a view that high enough to take into account the relationships between once disparate lines of business. Each line of business or department may have met the letter and spirit of the law in regard to auditing their compliance to regulatory requirements, but because an organization is a culmination of many departments and possibly many lines of business, those very relationships create exposures not assessed by their individual auditing efforts. Also, with the advent of regulatory agencies assessing a business's aggregate operational risk, there needs to be a way of looking at the organization as a whole rather than its many parts. The following three figures help to make the point.

Figure 4 shows a series of threats and vulnerabilities (left) and audit activities that might be carried out to assess and verify the strength of the organizations security controls (right). Please note that the relationship between the threats and associated audit measures is arbitrary in this example. The intention is to

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

show that a variety of audit activities are performed to assess a broad number of issues, not which audit functions apply to which threats and vulnerabilities.

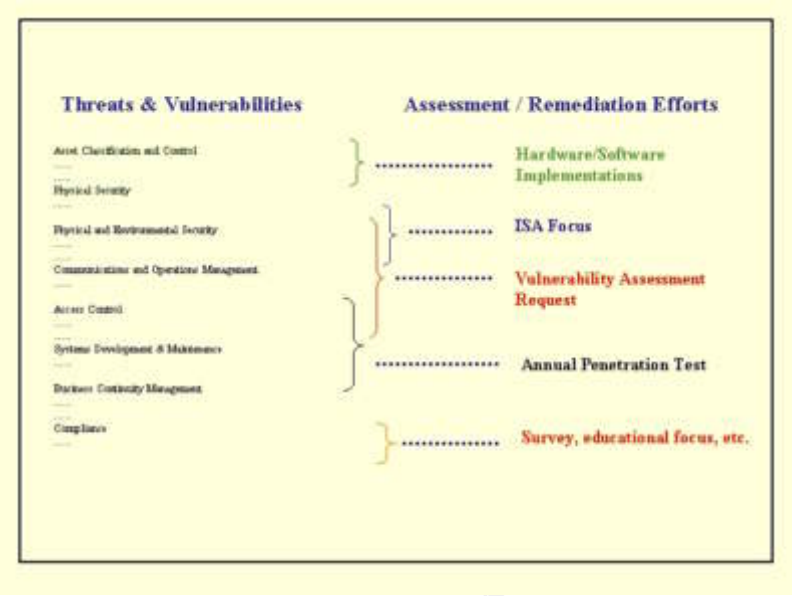


Figure 4

Figure 5 identifies exposures and duplicate audit activity. Lines A and B show that, though there are several audit activities taking place, there may be gaps in what is assessed and verified. Again, tried and true auditing approaches of the past may not be taking new relationships into account and critical exposures may go untested. Secondly, different parts of the organization, if not coordinated, may endeavor to respond to the same threats and vulnerabilities. Ellipse C represents three separate efforts likely to be assessing many of the same controls.

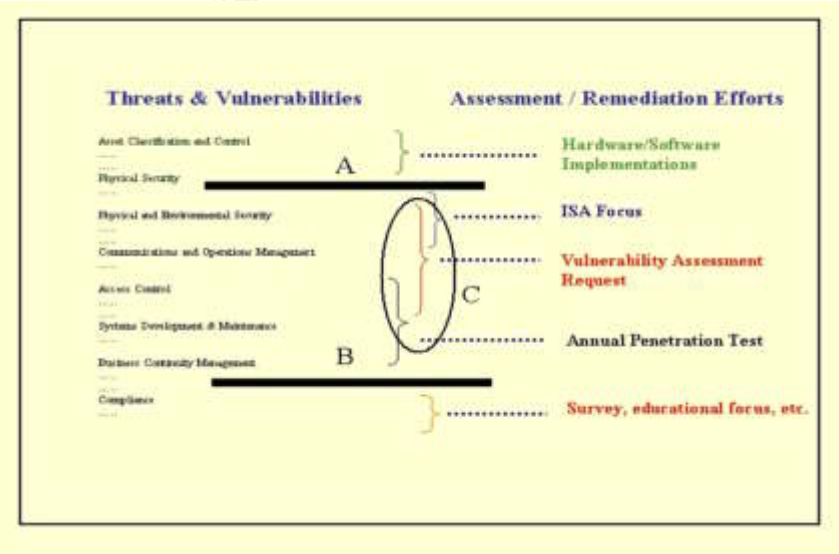


Figure 5

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Finally, figure 6 shows that audits conducted across an organization without high level of coordination do not assess an organization's operational risk no mater how many audits are performed. The single auditing perspective is a must to first, understand all that must be attended to and second, gather all related data to determine the soundness of the organization's security controls.

Perhaps just as important is opportunity cost of independent audit activity. Even if there were no verification gaps (lines A & B) or duplicitous activity (ellipse C) sharing and leveraging knowledge between so many efforts is non-existent. Important audit findings, mitigating controls, and remediation solutions developed by one effort are lost to the others.

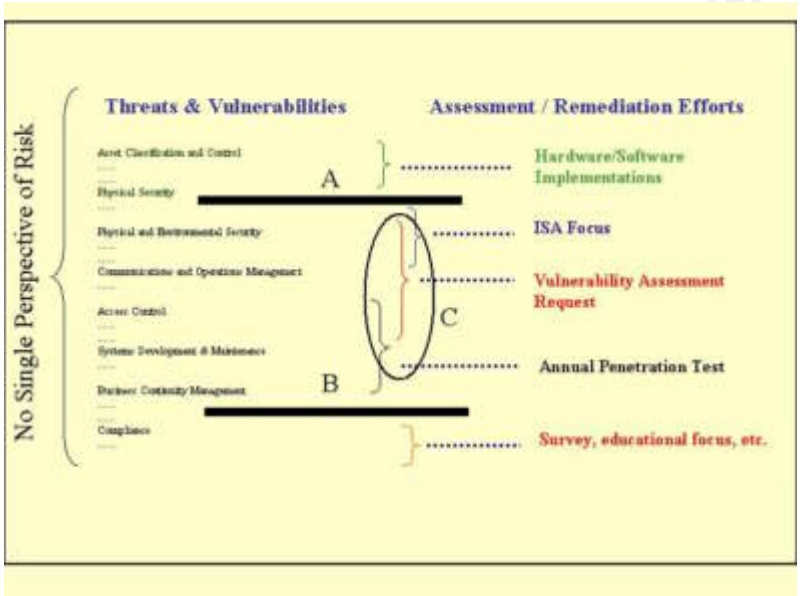


Figure 6

To be most effective, the controls must be tied back to the enterprise information security policy. Each control should be traceable to the policy statement or statements it supports. Its relationship to the policy is what gives it "teeth;" the means to enforce the use of a control when it's less than convenient to do so.

The fact is, security controls cost money to create and implement. Therefore, the business must be able to justify and support such security expenditures. However, determining what to protect and how to protect it is not an exact science. Estimating the loss due to a given exposure is often the culmination of subjective opinions and best guesses. All affected parties may agree that a given resource should be protected, but may differ to the extent (expense) they are willing to go to protect it. It's likely the parties furthest from the threat or who have no direct ownership of the resource will be less enthusiastic about mitigating all known vulnerabilities. But in this evermore-connected world it's increasingly important that an organization consider threat mitigation from the enterprise perspective: an exposure to one part is a threat to all parts.

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

So the question becomes how to arrive at a consistent, less subjective means of assessing threat and the appropriate response to it. This is, of course, what the study of risk management is all about, but it is mentioned here to show the connection between the information security policy and security controls available to an organization. The Procurement Guide for Financial Institutions summarizes the GLBA[2] guidelines in regard to policy this way: "To achieve compliance with U.S. Federal requirements the compliant organization needs to establish written policies and procedures…commensurate with the sensitivity of the information as well as the complexity and scope of the financial institution and its activities" (Dahl/Mattsson, p. 3). In other words, the policy establishes for the organization consistent guidelines for what to protect and the extent it will be protected.

Summary

Auditing has been around for a long time and auditing practices, developed over decades, have been proven effective for the systems they assess. Yet, regardless of how effective these approaches have been they themselves need to be assessed against the new environment of e-Business. E-Business is not just a new way of doing old business, it's a new "click-in" alternative that has brought with it a whole new economy; an economy of "connectedness" that allows business to be conducted virtually anytime, anywhere, by anybody.

While the opportunities in this new world are vast the potential for abuse is equally so. According to Internet Security Systems, Inc., 300 new security issues are introduced every month (Niccolai, p. 2). Staying abreast of and responding to so much threat activity requires the ability to act decisively. Limited resources must be applied to the high-risk, mission critical business operations and a single perspective of what needs protecting and the controls available to protect it is required to respond effectively.

The immaturity of the technology and the general difficulty in having to deal with securing a "borderless" space are challenging enough. But add to that the fact that constituent parts of a business or organization, once isolated from one another exposure-wise, now have whole new sets of vulnerabilities to consider. Namely, vulnerabilities once borne by disparate parts of the organization are now, at least to some degree, borne by all. Still other vulnerabilities are created by new internal and external relationships: new groups of people are sharing the same network and sometimes handling the same data.

The critical element expressed in this paper is the fact that the overall business connectedness requires a change in the auditing perspective. Organizational adjustments have to be made to raise the level of auditing sponsorship in response to the breadth of exposure. It is not an undoing or a major overhaul of auditing in general, but rather the addition of an auditing view from a higher perspective; a view that encompasses all of the new relationships. And, because

[2] GLBA: Gramm-Leach-Bliley Act

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

it is a wide perspective, involving so many elements within the organization, it will not happen on its own, but will require deliberate action: a strategy.

© SANS Institute 2003, Author retains full rights

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Bibliography/Resources

Bardwick, Judith. In Praise of Good Business. John Wiley & Sons, Inc. New York, NY. 1998. 3 – 19.

Basel Committee on Banking Supervision. "Overview of the New Basel Capital Accord." May 31, 2001. URL: http://www.bis.org/publ/bcbsca02.pdf

Bennett, Madeline. "Virus costs keep rising." IT Week. March 3, 2003
URL: http://www.vnunet.com/News/1139852

Dahl, Ulf. Mattsson, Ulf. "Privacy Compliance Procurement Guide for U.S. Financial Institutions." Itsecurity.com. May 6, 2002
URL: http://www.Itseurity.com

Ellul, Jacques (1990): *The Technological Bluff.* Grand Rapids, MI: Eerdmans
Ellul, Jacques. The Technological Bluff. Translated by Geoffrey W. Bromiley. Grand Rapids, Mich.: William B. Eerdmans Publishing Company, 1990.
Out of print but available at
URL: http://www.jesusradicals.com/main/library/ellul/bluff/Bluff.html

Huber, Elizabeth. Cook, Hudson. "Identity Theft: Consumers, Creditors & Criminals - Civil and Criminal Enforcement." November 12, 2002. The State Bar of California Business Law Section Financial Institutions Committee and the Beverly Hills Bar Association.
URL: http://www.couselorlibrary.com/articles/article32.pdf

Information Security Forum (ISF). "Standard of Good Practice." 2001.
URL: http://www.isfsecuritystandard.com

ISO/IEC 17799. "Information technology – Code of practice for Information security management." First edition. December 12, 2000.
URL: http://www.iso.ch/

Niccolai, James. "Report finds 37% jump in security incidents."
IDG News Service. April 4, 2003. URL:
http://www.computerworld.com/securitytopics/security/holes/story/0,10801,80049,00.html

SANS Institute, The. SANS Security Essentials V: Windows Security Windows Auditing. 2003. Section 6, page 8.

Shapiro, Carl. Varian, Hal. Information Rules: A Strategic Guide to the Information Economy. Harvard Business School Press. 1999.

Tauzin, W.J., Dingell, John D. "CRITICAL INFRASTRUCTURE PROTECTION Challenges for Selected Agencies and Industry Sectors." February 2003.

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

URL: http://www.gao.gov/cgi-bin/getrpt?GAO-03233

Zeichner, Lee M., Almosd, Robert. Zeichner Risk Analytics. "STATE IMPLEMENTATION OF FEDERAL CYBER-SECURITY REQUIREMENTS, States Continue to Lag Behind Federal Government and Industry Progress." 2002-2003,
URL: http://www.zra.com/docs/summaryReport.pdf

© SANS Institute 2003, Author retains full rights

Submitted by Stu Milus, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: April 18th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Abu Dhabi 2014	**Abu Dhabi, AE**	**Apr 26, 2014 - May 04, 2014**	**Live Event**
US Cyber Crime Conference	**Leesburg, VAUS**	**Apr 27, 2014 - Apr 28, 2014**	**Live Event**
SANS Austin 2014	**Austin, TXUS**	**Apr 28, 2014 - May 03, 2014**	**Live Event**
Security Leadership Summit	**Boston, MAUS**	**Apr 29, 2014 - May 07, 2014**	**Live Event**
SANS Security West 2014	**San Diego, CAUS**	**May 08, 2014 - May 17, 2014**	**Live Event**
SANS Secure Europe 2014	**Amsterdam, NL**	**May 10, 2014 - May 24, 2014**	**Live Event**
SANS ICS410 London 2014	**London, GB**	**May 12, 2014 - May 16, 2014**	**Live Event**
SANS Melbourne 2014	**Melbourne, AU**	**May 12, 2014 - May 17, 2014**	**Live Event**
SANS Malaysia @MCMC 2014	**Cyberjaya, MY**	**May 12, 2014 - May 24, 2014**	**Live Event**
SANS Bahrain May 2014	**Manama, BH**	**May 17, 2014 - May 22, 2014**	**Live Event**
AUD307: Foundations of Auditing Security and Controls of IT Systems	**Oklahoma City, OKUS**	**May 21, 2014 - May 23, 2014**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**May 26, 2014 - May 31, 2014**	**Live Event**
Digital Forensics & Incident Response Summit	**Austin, TXUS**	**Jun 03, 2014 - Jun 10, 2014**	**Live Event**
SANS Rocky Mountain 2014	**Denver, COUS**	**Jun 09, 2014 - Jun 14, 2014**	**Live Event**
SANS Pen Test Berlin 2014	**Berlin, DE**	**Jun 15, 2014 - Jun 21, 2014**	**Live Event**
SEC511 Continuous Monitoring and Security Operations	**Washington, DCUS**	**Jun 16, 2014 - Jun 21, 2014**	**Live Event**
SANS Milan 2014	**Milan, IT**	**Jun 16, 2014 - Jun 21, 2014**	**Live Event**
SANSFIRE 2014	**Baltimore, MDUS**	**Jun 21, 2014 - Jun 30, 2014**	**Live Event**
SANS Canberra 2014	**Canberra, AU**	**Jun 30, 2014 - Jul 12, 2014**	**Live Event**
SANS Capital City 2014	**Washington, DCUS**	**Jul 07, 2014 - Jul 12, 2014**	**Live Event**
FOR518 Mac Forensic Analysis	**San Jose, CAUS**	**Jul 07, 2014 - Jul 12, 2014**	**Live Event**
SANS San Francisco 2014	**San Francisco, CAUS**	**Jul 14, 2014 - Jul 19, 2014**	**Live Event**
SANS London Summer 2014	**London, GB**	**Jul 14, 2014 - Jul 21, 2014**	**Live Event**
FOR518 Mac Forensic Analysis	**OnlineVAUS**	**Apr 22, 2014 - Apr 27, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**