

# Strategic Alignment of IT & Security - Yield Compliance by Default.

## Table of Contents

What is Your Institution's Culture	1
Adopt a Culture of Continuous Risk Management	2
Who is in Charge?	5
Where Do You Go From Here?	5

January 2007



This paper provides forward looking thought leadership and recommendations on strategic, operational, and tactical activities to help you properly align the people, processes and technology infrastructure to work in harmony and create a cost effective and continuous risk management culture throughout the enterprise.

## WHAT IS YOUR INSTITUTION'S CULTURE?

Financial institutions are traditionally known for prudent and extensive security precautions. In today's inverted security environment, however, traditional perimeter focused security practices are not enough. An internal security black hole has emerged that requires immediate attention – insider ignorance, errors, and fraud.

Many institutions are at different stages of building on their traditional point-in-time perimeter security practices and evolving to adopt a culture of continuous risk management.

For example, some institutions have adopted and are enforcing a policy of continuous risk management and are realizing the benefits of reducing the head count for trouble shooting activities and reallocating those resources to revenue generating activities. These institutions have on-demand updated patch and vulnerability notification; a verifiable security posture; an ability to alert key personnel of a vulnerability or security event that requires attention; and remote access to just-in-time reporting through a secure web page to allow access to key monitoring information from anywhere at anytime. Such institutions can report their compliance status in an instant; they are aware of vulnerabilities before problems occur; and require fewer resources to prevent, detect, and respond to problem events.

Conversely, there are institutions that have not aligned automated assessment, monitoring, alerting, compliance, and training best practices throughout the organization. They have not adopted a culture of continuous risk management. Such institutions continue to struggle with reactive security measures, over-allocated resources for trouble shooting vulnerabilities and security events, and enforcing compliance.

Both types of institutions face similar threats and vulnerabilities. However, only those institutions that adopt a culture of continuous risk management can cost effectively reduce liability and enhance their ability to respond rapidly to protect the institution, its customers, and business partners from today's internal and external threats and vulnerabilities.

The risks are too great for no action! Network vulnerabilities, weak internal controls, and erroneous or fraudulent exposure of sensitive information can expose the institution to substantial financial loss<sup>1</sup>, damage to its reputation, weaker shareholder value, regulatory and civil fines and enforcement actions<sup>2</sup>, and significant business disruption in responding to such events.”

“An automated ability to assess vulnerabilities; monitor the security posture; alert key personnel to trouble; publish policies; remind employees to stay current and acknowledge policy awareness; and track and enforce internal compliance and acknowledgement of corporate policies will position an institution favorably for its next audit or regulatory examination. Implementing industry recognized best practices will position it with a strong posture for the next wave of audits, attacks, and a lower cost of operation.”

This paper provides forward looking thought leadership on the common aspects of many of today's information security and technology risk management initiatives that have evolved from cross-industry recognized best practices. The best practices of yesterday that were recognized by a few are now today's mandates for the many. Early adopters of these best practices realized that they could successfully address multiple concerns with a simple yet thorough approach to automation of risk management. By adopting a culture of continuous risk management, they have achieved compliance by default - not as a separately funded project for each compliance mandate. This

---

<sup>1</sup> According to an October 2006 study from Ponemon Institute, the average cost of a data breach is \$182 or more per data record. Notification of customers was a small part of this cost. A higher portion of this cost is for addressing customer retention with telephone and incentive campaigns to encourage customers to stay with the company.

<sup>2</sup> In September 2006, Gartner published a case study that put the cost of a data breach above \$350 per record. The higher costs were from loss of business and fines and consumer restitution.

“We are operating in an **inverted security** environment, where customers and business partners are allowed access into our networks and employees are allowed to transfer sensitive customer and corporate data out of our networks. All forms of sensitive information (financial, corporate, and personal) are moving across the network.”

*Paul Reymann  
CEO, ReymannGroup, Inc.*

compliance by default strategy allows them to capitalize on the common theme of best practice that is the inherent nature of many regulations.

“Simplifying regulatory compliance is as easy as aligning your compliance efforts and operational efficiency goals and realizing that they are not mutually exclusive. They are the same.”

Whether your institution has a strong risk management program or looking for ways to improve, this paper will provide strategic, operational, and tactical recommendations to help you properly align the people, processes and technology infrastructure to work in harmony and create a cost effective and continuous risk management culture throughout the enterprise.

“Such institutions can manage risk more effectively and enable compliance with key laws, rules, and policies, while facilitating a more productive use of resources and a lower cost of operations – freeing up resources to create efficiency, revenue generating opportunities, and new value.”

#### ADOPT A CULTURE OF CONTINUOUS RISK MANAGEMENT.

A prudent and continuous information security and technology risk management strategy requires all business units (e.g., operations, lending, technology, compliance, human resources, and others) to work together to replace the traditional silos of inefficient communication and operation with open and effective lines of communication in managing compliance-, technology-, and enterprise-risk. In short, the institution must migrate to a business paradigm in which everyone is made accountable and more self-aware of his and her duties and responsibilities and how he or she influences the success and security of the enterprise.

All financial institution management and personnel must remain alert to emerging threats and vulnerabilities. Traditional security practices must be updated and supplemented with automated capabilities for:

Traditional practices must be updated and supplemented with automated capabilities for:

- Real-time vulnerability -
  - Assessments.
  - Monitoring.
  - Alerts.
- Policy monitoring and enforcement.
- Compliance monitoring.
- User training.
- And much more.

#### *Real-time security and activity monitoring.*

A static security program provides a false sense of security and will become increasingly ineffective over time. Monitoring and updating the security program is an important part of the ongoing cyclical security process. Institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls.

Each financial institution should gain assurance of the adequacy of its risk mitigation strategy, operations, and tactics. Security personnel and system owners should monitor for new vulnerabilities and develop appropriate mitigation solutions to address them. Examples include:

- Establishing an effective process that monitors for vulnerabilities in hardware and software and establishes a process to install and test security patches.
- Maintaining up-to-date anti-virus definitions and intrusion detection attack definitions.
- Providing effective oversight of service providers and vendors to identify and react to new security issues.

“**Security monitoring** focuses on the activities and condition of network traffic and network hosts.”

“**Activity monitoring** is primarily performed to assess policy compliance, identify non-compliance with the institution’s policies, and identify intrusions and support an effective intrusion response. Because activity monitoring is typically an operational procedure performed over time, it is capable of providing continual assurance.”

*Source: FFIEC July 2006  
Information Security Booklet.*

- Monitoring network and host activity to identify policy violations and inappropriate behavior.
- Monitoring host and network condition to identify unauthorized configuration and other conditions, which increase the risk of intrusion or other security events.
- Analyzing the results of monitoring to accurately and quickly identify, classify, escalate, report, and guide responses to vulnerabilities and security events.
- Responding to intrusions and other security events and weaknesses to appropriately mitigate the risk to the institution and its customers, and to restore the institution's systems.

#### *Real-time vulnerability assessments.*

Institutions must establish an ability to continuously look for vulnerabilities in a network that expose it to risk of unauthorized activity, degradation in performance, or other unwanted threat events that could cause harm to the confidentiality, integrity, or availability of information or information systems. Vulnerabilities can be characterized as weaknesses in a system, or control gaps that, if exploited, could enable unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Vulnerabilities are generally grouped into two types: known and expected. Known vulnerabilities are discovered by testing or other reviews of the environment, knowledge of policy weaknesses, knowledge of inadequate implementations, and knowledge of personnel issues. Adequate and continuous testing is essential to identify many of these vulnerabilities.

#### *Real-time vulnerability alerting.*

The sophistication of today's zero-day threats creates an immediate and enterprise-wide problem for an institution, its customers, and business partners. Many of these zero-day threats are designed to exploit known vulnerabilities in a network infrastructure and its systems. A rapid response capability to identify vulnerabilities and alert the necessary personnel is crucial in helping to prevent or remediate such threats. The goal of real-time vulnerability alerting is to allow the institution to execute a rapid response, which avoids or minimizes damage to the institution and its customers. The response primarily involves people rather than technologies. The quality of the response is a function of the institution's culture, policies and procedures, and training. Preparation determines the success. This involves defining the policies and procedures that guide the response, assigning responsibilities to a variety of individuals, providing appropriate training, and formalizing information flows among all parties. Responding to vulnerabilities can typically include expertise and participation from many different areas in the institution – management, legal, compliance, operations, human resources, and information technology.

#### **TraceMonitor™**

TraceMonitor™ notifies you immediately of server interruptions and if ANY of your files are changed. It helps you to protect sensitive internal files such as policy or personnel files, configuration or web files, network and email files, and more.

#### **TraceAssess™**

TraceAssess™ is an automated vulnerability assessment tool that evaluates your network for security risks and produces intuitive reports for executives and staff.

TraceAssess™ identifies vulnerabilities and tracks patches through remediation to ensure proper security posture and verified remediation.

#### **TraceAlert™**

TraceAlert™ is a vulnerability and patch alerting service. It greatly reduces the time to research and respond to security vulnerabilities that affect your network environment.

TraceAlert™ dramatically increases your ability to maintain a secure network. It delivers real-time vulnerability information to all key personnel – empowering you to respond rapidly to vulnerabilities.

*Policy monitoring and enforcement.*

All employees must formally acknowledge his or her understanding and acceptance to follow board approved policies. A successful policy enforcement program, however, will require this process to repeat many times throughout an employee’s career with the institution. Senior management should support strong ongoing security policy awareness and compliance. Management and employees must remain alert to operational changes that could affect security and actively communicate issues with security personnel. Business line managers must have responsibility and accountability for maintaining the security of his or her personnel, systems, facilities, and information. Everyone must be kept aware and educated, as the threats and vulnerabilities change that can affect the safe, sound, and secure day-to-day operations.

*Compliance monitoring.*

In this decade of compliance mandates, institutions need to have the ability to proactively know when user violations occur, take necessary remediation and enforcement action, help mitigate the risk of fraud, avoid financial loss, minimize the loss of productivity, and manage damage to the institution’s brand and reputation.

Senior management should require periodic self-assessments to provide an ongoing assessment of policy adequacy and compliance and ensure prompt corrective action of significant deficiencies.

A prudent compliance monitoring program will help the institution to:

- Know which regulations apply.
- Know when regulatory updates occur.
- Track and report formal awareness and training of all employees.
- Require all employees to be knowledgeable of compliance mandates.
- Provide reports to the board and executive management on compliance status.
- Incorporate compliance responsibilities into individual and business unit performance plans.

*User training.*

Financial institutions need to educate users regarding policies and his or her security roles and responsibilities. Training should support security awareness and strengthen compliance with security policies, standards, and procedures. Ultimately, the behavior and priorities of senior management heavily influence the level of employee awareness and policy compliance, so training and the commitment to security should start with senior management.

“Training materials for desktop and workstation users would typically review the acceptable use policy and include issues like desktop security, log-on requirements, password administration guidelines, etc. Training should also address social engineering and the policies and procedures that protect against social engineering attacks. Many institutions integrate a signed security awareness agreement along with periodic training and refresher courses.”

**TracePolicy™**

TraceSecurity helps you to create, distribute, modify, manage, and enforce your policies.

As policies are posted, users are automatically notified.

Management can track who has and has not read policies, memos, and other electronic information.

**TraceComply™**

TraceComply™ enables you to track your compliance status across the entire organization for industry, local, federal, and international rules and standards.

TraceComply™ users take an online compliance interview on the information security soundness of key functional areas such as: Physical; Technical; Managerial; and Operational.

TraceSecurity helps organizations manage complex security regulations and stay up-to-date.

**TraceTraining™**

TraceTraining™ offers comprehensive and personalized online training courses enabling your employees and customers to learn at their convenience. It allows you to track participation, completion, and test scores.

## WHO IS IN CHARGE?

Everyone must be accountable! The ultimate responsibility for pulling together the human and technology resources among information technology staff, human resources, security personnel, back-office and front-line staff, executive management, and board members sits on the desk of the Information Security Officer<sup>3</sup>.

Everyone needs to become aware of his and her responsibilities for adopting daily security practices to help mitigate vulnerabilities and the risk of unauthorized use or breach of sensitive information or network resources. Prudent and educated user behavior must also be supported by an enterprise-wide infrastructure of automated and proactive risk management solutions that help prevent, detect, and respond to network and user vulnerabilities.

However, adopting a successful culture of continuous risk management requires a top-down and bottom-up awareness and acceptance of responsibility among the Board, executive management, and all staff. Each business unit manager's acceptance of his and her portion of the risk, duties, and responsibilities is an imperative. Such responsibility and pride of ownership must also be imbedded throughout the organizational chain-of-command to the back-office and front-line personnel.

The role of the compliance officer will also change. An automated capability to manage compliance, distribute and maintain policies, assess and monitor for vulnerabilities, and train employees will enhance the compliance officer's role - managing risk to the enterprise, not just compliance.

## WHERE DO YOU GO FROM HERE?

Improve your organization's security posture.

In today's complicated and rapidly changing networked environments, existing security technologies such as anti-virus, firewalls and intrusion detection are not enough to protect your institution's resources from the constantly emerging vulnerabilities and threats. Institutions must become proactive in dealing with security.

TraceSecurity Compliance Manager™ is an ASP-based product that combines asset database information, policy monitoring, vulnerability information, and compliance surveys to determine if an institution is meeting regulatory and compliance standards. It gives you a real-time view of your policy and network environment and provides actionable alerts, recommendations, and remediations to help you prioritize resources.

TraceSecurity Compliance Manager™ is comprised of five unique applications:

1. [TraceMonitor™](#) - Immediate notification of server interruptions and file changes.
2. [TraceAssess™](#) - Ongoing, automated vulnerability assessment.
3. [TraceAlert™](#) - Real-time vulnerability alerting information.
4. [TracePolicy™](#) - Policy tracker for policies, memos, and other electronic information.
5. [TraceComply™](#) - Evaluates policies for compliance with FDIC, FFIEC, GLBA, HIPAA, NCUA, and OCC regulatory mandates.

If you would like to learn more about solutions that can help you to create a competitive business advantage and comply with today's regulatory mandates, contact the ReymannGroup to talk with one of our industry subject-matter experts by calling (410) 878-2744 or visit [www.complianceandbeyond.com](http://www.complianceandbeyond.com).

If you would like to try the TraceSecurity software solutions discussed in this paper, go to [www.tracesecurity.com](http://www.tracesecurity.com) to sign up for a free evaluation or call one of the TraceSecurity representatives today for complete information at (225) 612-2121.

---

<sup>3</sup> The FFIEC July 2006 Information Security booklet states that the Information Security Officer should “directly manage or oversee the risk assessment process, development of policies, standards, and procedures, testing, and security reporting processes.”

## **ReymannGroup, Inc.**

1908 Blue Ridge Road  
Edgewater, MD 21037  
USA

Phone: (410) 956 7334  
Fax: (410) 956 7338  
Email: [info@reymanngroup.com](mailto:info@reymanngroup.com)

## **TraceSecurity**

7145 Florida Blvd.  
Baton Rouge, LA 70806  
USA

Tollfree:(877) 275 3009  
Phone: (225) 612-2121  
Fax: (225) 612 2269  
[www.tracesecurity.com](http://www.tracesecurity.com)

ReymannGroup, Inc. provides finance, healthcare, retail and manufacturing subject matter expertise. Our firm helps companies evaluate their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. ReymannGroup provides customers with independent, highly-qualified professionals, authors of regulations and books, and subject matter experts familiar with financial, healthcare, retail and manufacturing industry regulations and best practices.

Privately-held TraceSecurity is a leading provider of on-demand security compliance software and services. The company's solutions help customers satisfy national and international data security compliance requirements mandated by such regulations as Sarbanes-Oxley, GLBA and HIPAA. Over 500 customers in the financial services, insurance, energy, government, manufacturing and services industries rely on TraceSecurity to continually monitor and improve the computer security of their companies. TraceSecurity's products and services include on-demand vulnerability and compliance assessment software, social engineering audits, comprehensive security assessments and security strategy consulting.

Headquartered in Baton Rouge, LA, TraceSecurity maintains offices in Houston, TX; San Diego, CA; and Portland, OR and an Advanced Technology Resource Center in Cupertino, CA. The company can be reached by phone at (225) 612-2121 or by email at [info@tracesecurity.com](mailto:info@tracesecurity.com).