



October 2009

**We've updated The Compass to compliment our new website design!**

See what else is new by **visiting us** on the web.

**Meet Experts of The Compass at the Following Events:**

*2009 Calendar of Events*

**10|14 WIB Annual Bank Technology & Security Summit, San Diego, CA**

**11|16 CA & NV Credit Union Leagues Annual Meeting & Convention, Las Vegas, NV**

#### **Archive Download**

*Download a printable PDF to share with colleagues or access **The Compass** archives:*

» The Compass, October 2009 - **Download** (PDF)

» The Compass - **Archives**

**Sign up to receive *The Compass* monthly.**

Not already on our mailing list? Our monthly newsletter will help you keep abreast of industry and regulatory developments for the financial industry. **Sign up now!**

#### **Contact us!**

We are constantly working to improve **The Compass** and appreciate your feedback! Send your comments to: **education@compushare.com**

#### **Rate this article!**

**Click here.** Your response will take less than 1 minute!

## **Assuring Compliance - Comprehensive Building Blocks to an Effective Information Security Assessment**

by **Ed Morales**  
**Risk and Compliance Engagement Manager**  
**Compushare, Inc.**

Information Technology risk prevention and mitigation are critical mandates that every financial institution is challenged with daily. A core component supporting effective risk prevention and mitigation is the annual Information Security Assessment. Every financial institution should have an annual Information Security Assessment performed by an independent third party vendor as part of their overall security program. An Information Security Assessment is designed to assess the current security controls within the institution, identify weaknesses and vulnerabilities in both technical and procedural processes, and, most importantly, provide a consultative analysis that includes recommendations and remediation.

#### **Choosing the Right Third Party Vendor**

Having an Information Security Assessment performed by a third party can benefit a financial institution by, not only addressing regulatory compliance concerns, but also in many cases identifying security holes the financial institution never knew existed. Having a second set of eyes to evaluate the security program, test for external and internal security controls and vulnerabilities, and review procedures can assist in determining where security needs to be strengthened and fortified. The consultative analysis included in the assessment may further assist a financial institution in determining how to spend their security budget.

Often, less than 10% of a financial institution's IT budget is spent on security. Therefore it is imperative, particularly in the current economic environment, that every dollar spent on security is spent wisely. Not all security assessments are alike; selecting the right vendor that tests and analyzes the proper controls is a critical step. The Information Security Assessment should be designed to not only identify weaknesses, but also to assist the financial institution in taking the appropriate corrective steps to mitigate or prevent identified risks. Remediation must be approached as a main component of the Information Security Assessment, not an afterthought.

#### **A Comprehensive Approach**

Compushare's Information Security Assessment offering is designed as a comprehensive program which includes the testing of key controls in systems and procedures, identification of weaknesses and vulnerabilities, consultative analysis, recommendations to address identified weaknesses and vulnerabilities, and any remediation work required to ensure the safety of the institution's network and systems. The current design of the program provides our clients with the assurance and added value that weaknesses are not only identified, but are also effectively corrected.

#### **Testing Physical Security Controls**

The institution should ensure that key testing components are addressed by the chosen third party vendor. The testing of physical security controls should be the first step in any assessment. All firewalls and technical controls put in place can be bypassed if someone can gain physical access to your data. A Physical Site Assessment looks at the physical security controls in place and should include a Social Engineering Test to see how employees react to strangers attempting to gain physical access to non-public areas of the financial institution. There may be exploitable vulnerabilities at the physical level of which the institution may not even be aware. For instance, on more than one occasion, Compushare Security Consultants have identified live data ports in publicly accessible areas of the branch. Social engineering attacks come from many fronts, so it is imperative that the testing mimics real life attacks. Social engineering via phone calls and email phishing tests should be included as a mandatory component of any security assessment. In recent news, the head of the FBI, Robert Mueller, nearly fell for an email

phishing attack from an email that appeared to come from within his bank. This sheds light on how almost anyone can fall victim to these types of attacks.

### **External Penetration Analysis**

Assessments should also include an External Penetration Analysis that looks at the public facing devices and network of an institution from an external perspective, including the institution's web site. Web sites are often not designed with information security in mind. An institution's web site serves not only as a public image for the institution; it is also, in many cases, an access point into the institution via the online banking page. Online banking entry points are regularly targeted for malicious intent. It is critical that the security assessment includes analysis of the financial institution's web site and verification to ensure that the site is GLBA compliant. Given the onslaught of attacks targeting web sites today, a proactive approach is to conduct a Deep Web Application Test that will help to identify any vulnerabilities that a hacker might try to exploit.

### **Testing Internal Security Controls**

The testing of Internal Security Controls is another core component of the Information Security Assessment. As the threats evolve, so must the assessment. Every computer with Internet access should be looked at as a potential gateway for incoming threats. Does your institution have the proper controls in place to mitigate risks at the workstation level? The testing and evaluation of all the security controls in place are essential to identifying and addressing these threats.

### **Risks From Inside Sources**

Additionally, the threat of malicious behavior from employees is a potential risk that should be factored into the equation. Does your security program have the proper mechanisms in place to identify and react to an attack or malicious action from an employee? A well developed Information Security Assessment will look at all vulnerability points to the financial institution at both the server and workstation levels, from both internal and external attack points.

These are just some examples of core Information Security Assessment components. The financial institution should determine which controls should be tested annually; here is a recap of items to consider:

- External Penetration Analysis
- Firewall Review
- Social Engineering/Email phishing
- Physical Site Assessment/Social Engineering
- Deep Web Application Scan
- Internal Vulnerability Assessment
- Windows Domain Policy Review/ User Account Setting Review
- Vulnerability Management – External/Internal

### **Testing Accomplished - Now What?**

Equally as important as the testing parameters are the consultative analysis and recommendations that the third party vendor provides. If the vendor does not provide any assistance with remediation of the vulnerabilities that they have identified, then they have completed only half the work. Many vendors will provide a cookie cutter Information Security Assessment solution at a low cost, only to charge a high premium for any remediation work to be performed.

Ultimately, the financial institution is responsible for evaluating the effectiveness of their security program, and the proper Information Security Assessment will help them accomplish their objective. The recommendations and remediation work performed should strengthen the institution's overall security infrastructure. Compushare's team of Security Consultants holds years of real world experience in, not only the information security and compliance arena, but also in community financial institution management. By including remediation in the overall package, our Information Security Assessment program is distinguished from other providers and unrivalled in the IT security market. Compushare understands that financial institutions are looking to make every IT dollar count. Institutions can rest assured that all security, compliance and remediation concerns are fully and expertly addressed through partnering with Compushare, with tangible value delivered to the institution through the assurance of a comprehensive solution.

###

Compushare delivers viable and proven solutions exclusively for community financial institutions including areas of information security, risk management, risk assessments, business continuity, business resumption, managed technology services and hosted messaging solutions. Learn more about our approach toward **Strategy**, **Safety**, **Soundness** and **Support**.

To learn more on how your institution can benefit from a comprehensive Information Security Assessment solution including Remediation, contact your Client Solutions Executive or [education@compushare.com](mailto:education@compushare.com).