

A Banker's Guide to Performing IT Risk Assessments

IT Security Compliance,
Risk & Audit Solutions

Objectives

This educational webinar will reveal:

1. New changes to FFIEC Guidance
- 2. Regulatory considerations for risk assessments**
3. Best Practices for risk assessments
- 4. A detailed 7-step risk assessment process**
5. Process considerations

New Changes to FFIEC Guidance

In response to the evolving threat landscape, the FFIEC has issued supplemental guidance to its 2005 “Authentication in an Internet Banking Environment”.

2005 Guidance Overview

- Promoted multifactor authentication as the primary control
- Provided minimal supervisory expectations
- No strict timetable for performing risk assessments

New Changes to FFIEC Guidance

The new FFIEC guidance provides clear expectations of financial institutions regarding authentication, layered security and other controls.

- Review/update risk assessment as new information becomes available, prior to launching new online services, or **at least every 12 months**
- Use risk assessment results to determine authentication techniques, layered security and other control elements
- Establishes minimum control expectations and identifies controls that are ineffective
- Establishes standards and elements for the institution's customer/client education and awareness program

New Changes to FFIEC Guidance

There is now a much stronger emphasis on an institution's risk assessment. Specific Supervisory Expectations include:

- Risk assessments performed, reviewed and/or updated **at least every 12 months**
- Risk assessments must account for **NEW AND EVOLVING THREATS**, both internally and externally
- Risk assessments must consider changes in how customers use **online systems**
- Updates must include considerations for security incidents that affect the industry
- Examiners will begin assessing in **January, 2012**

What that means to Banks

- **Banks without a current, comprehensive risk assessments must perform one by January, 2012**
- **Manual risk assessments will become exponentially more complex and time consuming**
- **Risk mitigation strategies can no longer rely on technology to provide adequate protection**
- **Banks must begin implementing customer awareness programs**

Regulatory Considerations

Since 1999, the Gramm-Leach-Bliley Act (GLBA) has required financial institutions to perform a risk assessment to identify the risks that could compromise data, and determine the potential impact of the risk.

- To protect against any anticipated threats
- Encompass all reasonable and foreseeable threats

Regulatory Considerations

According to the FFIEC IT Examination Handbook:

Financial institutions must maintain an ongoing information security risk assessment program that effectively:

- **Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;**
- **Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets; and**
- **Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.**

Regulatory Considerations

According to the FFIEC IT Examination Handbook:

- Risk assessments should be updated as new information affecting information security risks is identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change, or configuration change).
- At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered.

Beginning January, 2012, new FFIEC Guidance states that banks must perform, review and/or update risk assessments at least once a year

Risk Management Lifecycle



Overview of a Risk Assessment



A risk assessment is the first process in the risk management methodology.

A risk assessment should answer these questions:

- **What can go wrong?**
- **How can it go wrong?**
- **What is the potential impact?**
- **What preventative steps can be taken?**
- **How can it be stopped from happening again?**

How Risk Assessments Help an Organization

The results of a Risk Assessment are used to

- **Identify which assets are the most critical**
- **Gauge the overall level of risk to the IT systems**
- **Establish a basis for prioritization of risk**
- **Recommend courses of action to protect the assets at risk**
- **Establish appropriate controls for customer authentication and layered security**

Implications of NOT Having a Risk Assessment

- **Increased risk exposure by having insufficient or inadequate controls**
- **Waste money and resources by implementing unnecessary controls**
- **Unbalanced asset protection: may provide too much protection for low value/low risk assets, and not offering enough for high value/high risk assets**

Either scenario leads to inefficient allocation of resources and money, yet could be corrected by a proper risk assessment.

The 7 Steps of a Risk Assessment

Data Phase Gathering	Step 1 – Asset Classification Step 2 - Threat & Vulnerability Identification
Phase Analysis	Step 3 - Control Analysis Step 4 - Likelihood Determination Step 5 - Impact Analysis
Phase Reporting	Step 6 - Risk Determination Step 7 – Results and Recommendations

Step 1 – Asset Identification Classification

Establishes the scope of the risk assessment effort and provides detailed information about the types of assets that exist within the bank.



Questionnaires



Interviews



Documentation Review



Vulnerability Scanning Tools

**Data
Gathering
Phase**

Step 1 – Asset Identification Classification

Hardware / Software

- Servers
- Core Processing
- Online Banking
- Workstations
- Laptops
- 3rd Party Software
- Network Design

Facilities / Physical

- Server Room
- Data Center
- Backup Tapes
- Documentation
- Phone Closets
- File Cabinets

Step 1 – Asset Identification and Classification

Additional information includes

- **Functional requirements of the system**
- **Organizational security policy and architecture**
- **System network topology/architecture**
- **Users of the system**
- **Flowchart of information throughout the system**
- **Technical controls used for the IT system**
- **Management controls used for the system**
- **Physical and environmental security mechanisms**
- **Operational controls used for the IT system**
- **Environmental security implemented for the IT system processing environment**

Step 2 – Threat and Vulnerability Identification

What is out there putting us at risk?

- Identifying threat sources with the potential to exploit weaknesses in the system
- Establish a comprehensive listing of potential threats
- Tailored to the organization and its processing environment
- Common threats can be categorized into areas:
 - **Natural threats** (external floods, earthquakes, tornadoes, storms)
 - **Environmental threats** (internal floods, power failures, fires)
 - **Human threats** (social engineering, human error)
 - **Technical threats** (hackers, denial of service)

Step 3 – Control Identification & Analysis

What controls do we have in place to reduce risk?

Do these controls have the necessary components to operate effectively?

Control Categories

- **Access and Authentication**
- **Change Management**
- **Personnel Security**
- **Host Security**
- **Etc...**

Step 4 – Likelihood Determination

The likelihood that a potential vulnerability may be exploited by one of the threats that have been identified.

Factors to be considered:

- A threat source's motivation and capability
- Regional issues (weather, etc.)
- The location / exposure of the system or information

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable.
Moderate	The threat-source is motivated and capable, probability is of moderate level
Low	The threat-source lacks motivation or capability, probability is occurrence is low

Step 5 – Impact Analysis

The impact a particular threat would have on an organization:

Loss of Confidentiality – refers to the protection of information from unauthorized disclosure

Loss of Integrity – occurs if unauthorized changes are made to the data or IT system by either intentional or accidental acts

Loss of Availability – Loss of system functionality and operational effectiveness of a mission-critical IT system

Magnitude of Impact	Impact Definition
High	Exercise of the threat (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Moderate	Exercise of the threat (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the threat (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

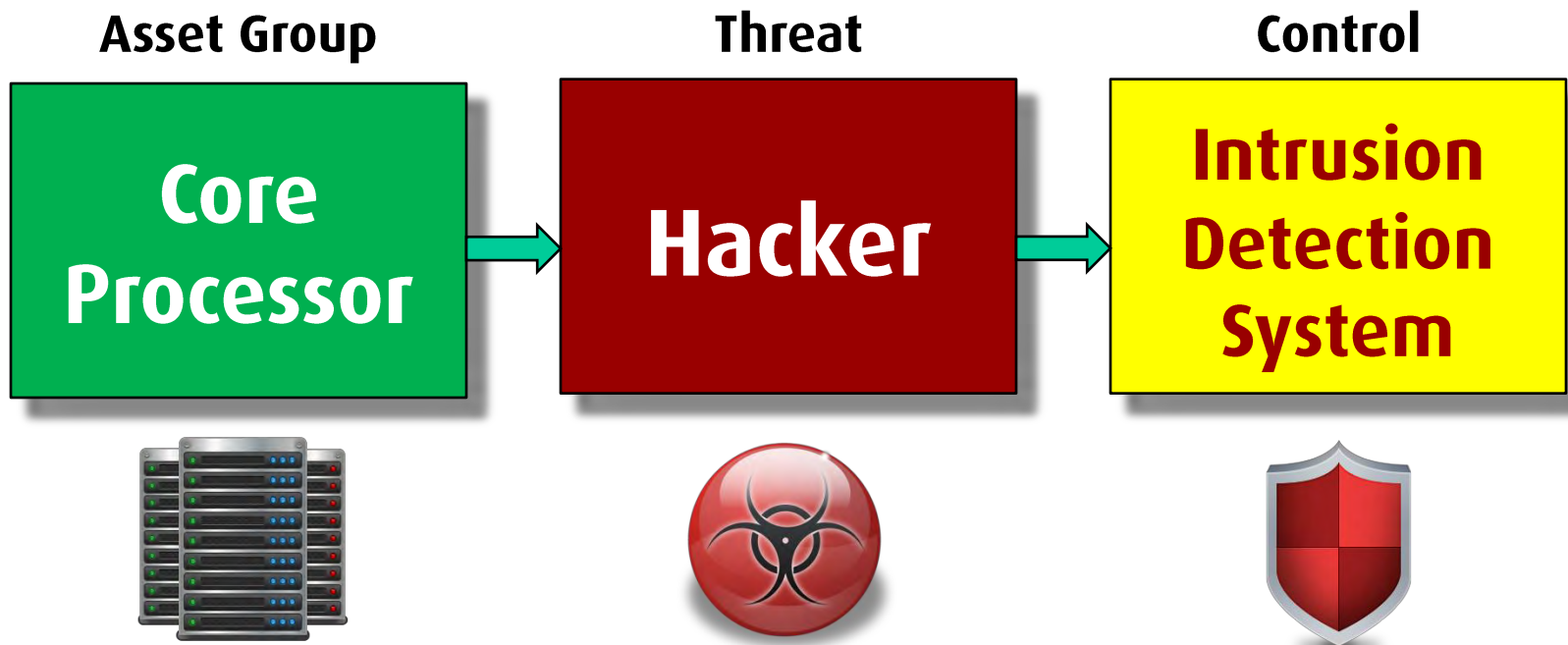
Step 6 – Risk Determination

The purpose is to assess the level of risk to the IT system.

The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The *criticality* of an asset
- The *likelihood* of a given threat
- The *magnitude of the impact* of the threat
- The *adequacy of security controls* for reducing or eliminating risk

Putting the Pieces Together



Step 6 – Risk Determination

Risk levels can be categorized by the following:

Risk Level	Risk Description and Necessary Management Action
High	If an observation or finding is evaluated as high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Moderate	If an observation is rated as moderate risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's authorizing official must determine whether corrective actions are still required or decide to accept the risk.

Step 7 – Recommendations and Results

Recommendations are essential for the risk mitigation process.

- **Identify & select appropriate controls that could mitigate or eliminate identified risk**
- **Reduce the level of risk to an acceptable level**
- **Identify, document, and justify areas of acceptable risk**

When issuing recommendations, consider these factors:

- **Effectiveness of recommended options**
- **Legislation and regulation**
- **Organizational policy**
- **Operational impact**
- **Safety and reliability**

Step 7 – Recommendations and Results

Results should be included in a formal report encompassing all risk assessment activities and documents the overall risk posture of the system.

- **Provides sufficient information so that management can make sound, risk-based decisions**
- **Used as a benchmark for risk-mitigation plans**
- **At a minimum, the report should describe the following:**
 - **Scope of the assessment based on the system characterization**
 - **Methodology used to conduct the risk assessment**
 - **Observations resulting from conducting the risk assessment**
 - **Estimation of the overall risk posture of the system**
 - **Recommendations to reduce risk**

Process Considerations

Manual solutions

- **Time consuming**
- **Manual entries of asset groups, threats, and controls**
- **Subjective**
- **Difficult to update and maintain, especially under the new FFIEC guidance**
- **Not always supportive of collaboration**

Process Considerations

Purpose built software solutions

- **Focus on risk, not calculations**
- **Pre-configured to reduce setup time**
- **Facilitates collaboration**
- **Gets to the detail without the overhead**
- **Automates where possible**

Summary

- **The goal of an institution in identifying and evaluating information risk should be to not only satisfy compliance, but to also protect the data of your company and customers/members**
- **This is done by having a clear view of where potential threats exist, the likelihood those threats could affect the organization, and how to eliminate or mitigate the risk**

Summary

- **A proper IT Risk Assessment should be a guide for internal decision making as it relates to the overall Information Security Program**
- Risk assessment should be thought of as an ongoing process, not as a one-time evaluation
- **Beginning in January, 2012, examiner's will verify a risk assessment meets the new FFIEC standards:**
 - Accounts for changes in internal and external threat environment
 - Changes in how customers use online banking systems and functionality
 - Accounts for security incidents affecting the bank or the industry

TraceSecurity Resources

Risk Assessment White Paper

Details the importance and scope of a risk assessment

Risk Assessment Worksheet

Guide for preparing for a risk assessment

FFIEC's Information Security Risk Assessment section

From the FFIEC's Information Security Booklet

FFIEC's Supplement to the Authentication Guidance

Download at www.tracesecurity.com/essentials

Contact Info:

Brady Justice
(225)-612-2121
brady@tracesecurity.com

sales@tracesecurity.com
(877)-275-3009

- Security Assessments
- Risk Assessment
- IT Security Audits
- Penetration Testing
- Social Engineering
- Security Training
- Application Testing

www.tracesecurity.com