Template

Purpose

- This is a "template" Awareness Training Procedure to be used as a "starting point" for the sake of helping you develop your own Awareness Program.

Copyright / Permission to Use

- Permission to use this document is conditional upon you receiving this template directly from an **infotex** employee, **infotex** website or e-commerce site, or an **infotex** workshop / training presentation.
- By using this template either in its entirety or any portion thereof, you acknowledge that you agree to the terms of use as dictated in the "Transfer of Copyright Agreement" located at copyright.**infotex**.com. This agreement establishes that when you customize this template to your specific needs, your organization may have copyright of the customized document. However, **infotex** retains copyright to the template. This agreement also establishes that you will not share this or any other template with third parties other than auditors and examiners. You may not transfer ownership of the customized documents to any other organization without the express written permission of **infotex**.

Instructions

- Make sure to read through the template carefully as not all situations will pertain to your organization. However, to assist you in customizing the document to your specific needs, we have attempted to color code areas that will need your special attention. Color coding is as follows:
    - All areas needing customization and/or consideration are in **red**.
    - Sections that are in **brown** are optional sections according to our definition of best practices. These sections may be removed if they do not match your needs.
    - Sections in **blue** are merely instructions or additional information for knowledge purposes and should be removed.
    - Sections in **green** are examples.
- Note that you should confirm that all text has been changed to "black" before considering this template final for your organization. If there are any sections in any other color than black, then all situations or customization has not been considered.

This section (Templates) may be removed once the document has been customized, for at that time we turn ownership of the customized document over to you.

Iterations:

Iteration #: 7
Date of This Iteration: 06/06/2013
Original Iteration: September 2005

Next Update Due: 11/19/2014

Insert Financial Institution Name / Logo

Awareness Training Procedure

(Approved During xx/yy/zz [IT Steering / IS Steering / IT Governance / Audit / EDP] Committee Meeting)

Classified: Internal Use
Contact if found: Name, Title
Name of Financial Institution
City, State

Procedure Scope

This procedure applies to all Name of Financial Institution's Board of Directors, Bank Management, Information Technology Team Members, and internal users.

The [IT Steering / IS Steering / IT Governance / Audit / EDP] is responsible for overseeing the development, implementation, and maintenance of this procedure. It should be reviewed at least annually to ensure relevant information is appropriately considered.

The [IT Steering / IS Steering / IT Governance / Audit / EDP] is responsible for enforcing this procedure.

For questions concerning this procedure, see the Information Security Officer.

Introduction

Information security permeates the organization, and thus an extremely important step in mitigating information security risk is to make the entire team aware of key issues related to information security. Buy-in at the management level will ensure proper enforcement of policies and procedures, as well as a cohesive, cost-effective approach to risk mitigation. Therefore, it is imperative that the Management Team and employees undergo many different levels and layers of awareness training throughout the calendar year. The following

Objective

The purpose of this document is to establish training procedures that apply to all Management Team members and employees of Name of Financial Institution that connect to Name of Financial Institution's computer system owned by Name of Financial Institution. It also documents the process used by the Information Security Officer to ensure appropriate information security awareness throughout the calendar year.

The Federal Financial Institutions Examination Council (FFIEC) indicates that the financial institution should use training, and awareness programs to promote understanding and increase individual accountability. [excerpt] The Awareness Training Procedure intends to comply with these guidelines articulated in the FFIEC's Management Handbook.

These procedures comply with the organization's Information Technology Governance Policy.

Employee Policy and Awareness

The weakest link in information security is people. To secure Name of Financial Institution's information system, a team approach must be taken that involves the cooperation and awareness of each and every employee. The Acceptable Use Policy addresses all policies, guidelines, and standards related to the employee (user). This policy is facilitated by periodic Information Security Awareness Training. There is also a signature form on file for all employees, as well as an Acceptable Use Policy Comprehension Test documenting the employees' understanding of these issues.

Information Security Awareness Training

One of the most critical components of a sturdy Information Security Strategy is the establishment of a thoughtful, periodic Information Security Awareness Training program. The content of this training differs and is tailored to deliver pertinent information to the Board of Directors, Bank Management, Information Technology Team Members, and users. Attendance to various training programs is mandatory for all personnel as defined below. The Information Security Officer is responsible for tracking attendance and reporting problems to supervisors.

Board of Directors:
The Board of Directors will be invited to sit in on annual User Awareness Training as a means of educating the Board on information related to the importance if information security (as well as the type of training being provided to the end-user).

Bank Management:
Any reports to the Board of Directors by the Information Security Officer should be shared with the Management Team for awareness purposes. The Incident Response Team will receive annual training centered around the Incident Response Plan. Meanwhile, [IT Steering Committee / IS Steering Committee / Audit Committee / EDP Committee] members will receive awareness training as part of the Risk Assessment updating process on an annual basis. The Management Team should annually approve provisions in the performance evaluation of employees related to information security best practices. Finally, the Information Security Officer will provide training as needed per the Information Security Strategy Calendar in order to assist the Management Team in the execution of various duties (such as vendor due diligence review, access authorization, data classification, etc.).

Technical Awareness Training:
Because the [Network Administrator / IT Manager / Technical Team] is so instrumental in both securing information assets as well as enforcing policy and configuring the system to enforce policy, it is imperative that a training program be developed to make the [Network Administrator / IT Manager / Technical Team] aware of the appropriate policies, procedures, tools, standards, and guidelines that must be followed. Annual training should be supplemented with comprehension testing as well as ongoing training. The [Network Administrator / IT Manager / Technical Team] should be involved in the annual process for updating security standards and other appropriate documentation.

Training for the [Network Administrator / IT Manager / Technical Team] should also include a review of the IT Audit program and, in particular, those tests and resources available related to technical vulnerability assessments, log monitoring applications, network configuration audits, etc.

User Awareness Training:
As the end-user is the "first line of defense" in an Information Security Strategy, training for the user is paramount. Name of Financial Institution utilizes the following five components in its Awareness Training Program for the end-user:

- Annual Acceptable Use Policy Training (GLBA Compliance): Each year, just after the Acceptable Use Policy is updated, all personnel who log into Name of Financial Institution's network will undergo full training of the Acceptable Use Policy. This training will include a "due diligence quiz" that documents that the user not only received the training, but understood key provisions of the policy.
- Monthly Awareness Reminders: Once per month, an e-mail message or payroll stuffer will be sent from the Information Security Officer related to a specific current information security related topic.
- As-needed and On-going Awareness Messages: As new issues, vulnerabilities, or policies arise, the Information Security Officer will send via e-mail or portal posts additional reminders and/or announcements. Throughout the year, as well as in advance of annual training, various awareness exercises may be conducted. To ensure proper reading of awareness messages, the Information Security Officer will be careful about what is sent out. Examples of the types of messages that can be considered will include:
    - Ongoing Policy Reminders.
    - Vulnerability Announcements and Ongoing Threats
    - Reminders about various security practices
    - Awareness Exercises such as pretext calling, phishing tests, etc.
- New Employees: As part of the new employee orientation, the most recent Acceptable Use Policy Training and Due Diligence Quiz will be delivered.

Customer Awareness Training:
The Information Security Officer will work closely with marketing personnel and web developers to ensure an adequate mix of identity theft prevention education is distributed to customers in the form of flyers, web page elements, and public announcements. In order to comply with the June 2011 Supplement to the FFIEC's 2005 Authentication Guidance, the Information Security Officer will maintain a "Customer Awareness Training Strategy" that will be updated annually. This strategy will comply with the supplement to the above guidance, released in June 2011.

Access Management Training:
The Management Team will be trained to be familiar with the orientation, termination, and background check procedures that are documented in the institution's Access Management Procedure. Furthermore, Data Owners will be taught the Data Ownership Policy as well as the access authorization review process that is required by that policy.

Risk Management Training:
The Management Team will be trained to be familiar with the ongoing and drill-down risk assessment procedures that are required by the institution's IT Governance Policy.

Training Plans

On an annual basis, the Information Security Officer will prepare the annual Board, Management, Technical, User, and Customer Awareness training plans and present that to the [CIRT / management team / Steering Committee / Board of Directors], including hiring third parties to assist with such training.

Information Security Training Points

Training will be job specific, and will often be based on procedures in the Information Security Program. The training materials will address all pertinent issues including the following:

- Board and Management Team:
  - FFIEC Requirements pertaining to Board Oversight of Information Security
  - Annual Report to the Board Requirements
  - Vendor Management Issues
  - Information Security Officer Job Description and Calendar of duties
  - Pertinent Risk Analysis results
  - Ongoing risk mitigation efforts
  - Major policy/procedure revisions
  - The Information Security Strategy Calendar
  - Current CIRT activities
  - Primary controls
  - Planned controls
- Technical Team:
  - Security Standards
  - Applicable Policies and Enforcement Requirements
  - IT Audit Program
  - BCP and BCP Testing Plan
  - Pertinent Risk Analysis results
  - Ongoing risk mitigation efforts
  - Security Standards
  - Primary controls
  - Planned controls
- User:
  - Current Acceptable Use Policy
  - Information Security Best Practices
  - Current trends in Information Security
  - Applicable regulations
  - Social engineering tactics
- Customer:
  - Customer Awareness Training Strategy
  - Customer Risk Assessment
  - High Risk / Commercial Customer Education Documents
  - General Customer Education Documents

Broadcast Awareness

All personnel will be trained to understand the latest attack methods, especially social engineering methods. Training will encourage users to "broadcast awareness" in the event that activities lead one to believe an information security attack is eminent or ongoing. This means that when an event is discovered, the user will immediately inform his/her supervisor, who will make sure all appropriate parties of the bank are aware of the incident. Depending upon the size of your bank, you may want to modify this language to fit your own situation.

Ongoing Awareness Training

The Information Security Officer is responsible for providing a steady stream of ongoing training to users, in the form of vulnerability announcements, security reminders, and awareness exercises.

Vulnerability Announcements

The Information Security Officer will develop reliable sources for reporting day zero exploits, ongoing attacks, and new vulnerabilities. The Information Security Officer is responsible for filtering such sources down to all users that is appropriate. Announcements and the method used to convey such announcements should be job specific as much as possible.

Security Reminders

The Information Security Officer is responsible for sending regularly scheduled security awareness reminders on a monthly basis to all users, and can send such reminders to just the management team or portions of the team (such as the CIRT, Technology Committee, Data Owners, etc.) as appropriate. Beyond monthly security reminders, the Information Security Officer must monitor policy enforcement issues and send reminders accordingly.

Awareness Exercises

The Information Security Officer is responsible for arranging various "awareness exercises" either performed as part of third party tests or internally. Such exercises should be used to measure as well as establish awareness. Proper metrics are important to demonstrate progress overtime. The exercises selected should be based on risk as measured by likelihood and impact.
Examples of exercises include:

- Pretext Calling
- Physical Breach Attempts
- Spear Phishing
- Password File Analysis
- Clean Desktop and Locked Workstation Walkthroughs

- Trash Can Reviews and Dumpster Diving

Awareness Training Presentations

There are various training presentations available which the Information Security Officer may use to kickoff program reviews, introduce annual reports, etc. They are as follows:

- User Awareness Training (presented to all users, including management team members)
- CIRT Awareness Training (presented annually to the CIRT)
- Information Security Risk Management Kickoff Meeting (presented at the beginning of the annual Risk Assessment)
- Board Awareness Training (provided annually to the Board of Directors in advance of the Annual Information Security Report to the Board)
- Vendor Management Program (presented in advance of the review of the Vendor Management Program)
- Data Ownership Program (presented to data owners as a kickoff to the Data Ownership Program Review)

Note: Not all of the above sessions are required, we're listing them in case you want to consider them.

Definition of Management Team

For the sake of this procedure and other procedures referring to "Management Team," the President / Information Security Officer / Compliance Officer has defined the Management Team as including the following positions:

- President
- Chief Executive Officer
- Chairman
- Chief Financial Officer / Controller / Accounting Manager (top position in accounting/finance business functions)
- Chief Operations Officer / VP of Operations / Director of Operations
- Chief Information Officer
- Information Security Officer
- Human Resources Director / Personnel Director (top position in this business function)
- Legal Counsel
- Compliance Officer
- Internal Auditor
- Marketing Director
- Purchasing Director
- VP of Retail
- Sales Manager
- Lending Manager
- List others

Program Review

Each of the eight information security programs (Asset Management, Business Continuity, Data Ownership, Incident Response, Risk Management, Security Standards, Awareness (Management, Technical, User, Customer), and Vendor Management) will be reviewed on an annual basis with appropriate stakeholders. The purpose of each review will be to update the programs in response to any deficiencies noted in audits and tests, account for personnel changes, consider new risks, threats, and vulnerabilities, and streamline the process wherever possible. The review process itself will make appropriate management team members aware of the policies and procedures inherent in each program.

Comprehension Tests

Each year, the Information Security Officer will design new comprehension tests based on the results of the Information Security Risk Assessment. The Information Security Officer is responsible for tracking test scores and reporting results to supervisors. The following tests resulted from the 2012 Risk Assessment:

- Management Awareness Training Comprehension Quiz
- Technical Comprehension Quiz
- User Awareness Comprehension Quiz (based on the Acceptable Use Policy)

Concluding Sections

The following sections may or may not apply to your institution, depending upon your own policy/procedure development protocols. However, we do strongly urge you to include the distribution list, policy owner, and policy reviewers sections for your convenience and to ensure appropriate review and training. Please remove this section.

Reporting to the Board of Directors

The [Information Security Officer / Internal Auditor] will report to the Board of Directors on an annual basis that all procedures listed above have been reviewed for completion, enforcement, and training. Specifically, this report will indicate that all procedures listed above have been updated. The report will list deficiencies related to enforcement of the policies and procedures above, as well as indicate the level of training provided to members of the various teams affected by the policies and procedures listed above.

The Board of Directors will also receive summary reports of examinations, audits, and other assessments of the risk inherent in information security as they are required.

Noncompliance

Violation of these procedures may result in disciplinary action which may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Name of Financial Institution's information resources access privileges, and civil and/or criminal prosecution.

Storage of Policies, Procedures and Standards

The Information Security Officer is responsible for maintaining current copies of all information security related policies and procedures. These will be stored [state method and location] and an electronic copy will be stored off-site [state location]. The electronic copy will be updated annually (in December) as well as on an as-needed basis any time there is a major revision of a particular policy or procedure.

Contribution to Control Objectives for Information Technology

Note: This section can be removed if the financial institution is not subject to CobiT compliance.
Enforcement of this policy contributes to the achievement of CobiT 5.0:

- APO02: Manage Strategy
- APO11: Manage Quality
- APO12: Manage Risk
- APO13: Manage Security
- BAI09: Manage Assets
- BAI10: Management Configuration
- DSS05: Manage Security Services
- DSS06: Management Business Process Controls

Procedure Training

The procedure owner and members of the [IT Steering Committee / Branchless Banking Committee / IS Steering Committee / IT Governance Committee / Audit Committee / EDP Committee] must review this procedure annually and hold discussions to ensure that everybody understands the provisions of this procedure, as well as the implications upon their job description responsibilities.

Procedure Owner

- Title Here

Distribution List

The following positions will receive this policy and any changes to this policy:

- [IT Steering Committee / IS Steering Committee / IT Governance Committee / Audit Committee / EDP Committee]
- Information Security Officer
- Management Team Members
- IT Auditor
- [Network Administrator / IT Manager]
- CIRT: Note that you may want to copy the CIRT/IRT even if you are distributing to Steering Committee.
- Board of Directors (if issued a portable device)
- Any user with issued or authorized portable devices as defined in this procedure.

Procedure Reviewers

- Titles Here

Related Policies / Procedures / Tools

- Acceptable Use Policy
- AUP Signoff Form
- Awareness Training Procedure
- Conflict of Interest Policy
- Customer Identification Program
- Identity Theft Prevention
- Information Security Officer Job Description
- Management Awareness Procedure
- Portable Devices Security Procedure
- Portable Devices Procedure Signoff Page
- Privacy Policy
- User Awareness Training Comprehension Test
- User Awareness Training Presentation

Revisions

- 05/25/12: John Doe, Information Security Officer