

### Risk Assessment And Your Credit Union

The buzzword these days in the credit union industry is “risk assessment.” The main focus on risk assessment most recently is in four highly visible areas: Bank Secrecy Act, Information Security Programs, Disaster Recovery and Business Continuity Planning, and E-Commerce. Examiners and Auditors alike are asking “Have you performed a BSA risk assessment? “Where's your IT risk assessment? Have you documented your risk analysis of member information? Third-party vendors? OFAC? Disaster Recovery plan? Business resumption plan?” Where do we start?

Let's start by defining “risk.” The National Institute of Standards and Technology (NIST) in its publication *Risk Management Guide for Information Technology Systems* defines risk “as the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence.” Put another way, risk is the potential that events (expected or unanticipated) may have an adverse impact on your credit union's earnings, capital, or credibility.

NCUA uses 7 categories of risk, which credit unions have become familiar with as part of the examination process. The four categories most pertinent to the areas of Bank Secrecy, Information Security, Disaster Recovery/Business Continuity, and E-Commerce include:

- ▶ **Transactional Risk:** Risks associated with failure to deliver services or products in the manner intended.
- ▶ **Reputation Risk:** Risks associated with negative public opinion.
- ▶ **Compliance Risk:** Risks associated with failure to comply with laws, regulations, prescribed practices, enforcement actions or ethical standards.
- ▶ **Strategic Risk:** Risk arising from adverse business decisions or improper implementation of those decisions.

The following sections outline the basics for a risk assessment in each area as well as provide insight as to

what Examiners and Auditors are looking for when they ask to see your documented risk assessment for the Bank Secrecy Act, Member Information, Disaster Recovery and Business Continuity Plan, and E-Commerce Activities.

**“...risk is the potential that events (expected or unanticipated) may have an adverse impact on your credit union's earnings, capital, or credibility.”**

#### Bank Secrecy Act/OFAC Risk Assessment

The FFIEC published its Bank Secrecy Examination Manual last summer, with an update in July 2006. This manual provides guidelines in terms of a risk assessment in the Bank Secrecy and OFAC areas. A risk assessment should be performed that takes into account each credit union's unique members, products and services, and geographic locations.

For credit unions, an analysis of the membership base should include asking some of the following questions:

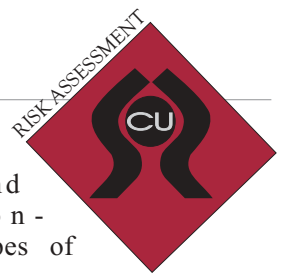
- ▶ Type of charter - does the credit union have a community charter, multiple SEG groups, or is it limited to one sponsor group?
- ▶ Are members and branches generally located in one central area or do they cross multiple state lines? Are branches and members located in foreign countries?
- ▶ Does the credit union open new accounts in any areas designated as high financial crime or high drug trafficking areas?
- ▶ What percentage, if any, does the membership consist of non-resident aliens or non-US citizens?
- ▶ Does the credit union have any transient members or groups such as university students, military personnel, etc.?
- ▶ Is membership limited to individuals or does the credit union also offer business accounts, organizational

accounts, and other “non-individual” types of accounts?

- ▶ Are any of the credit union's business accounts cash-intensive businesses or have the potential to be cash-intensive businesses?
- ▶ Can prospective credit union members apply for membership by mail or via the Internet or must they come into the credit union to establish an account?

Once the credit union has identified various risk groups within the membership, a risk ranking should be assigned to each group (such as low, medium, and high). Then current procedures for each risk group should be analyzed to determine if extra due diligence is required for new account opening and whether ongoing monitoring for suspicious activity is necessary.

The products and services a credit union offers should also be analyzed and assigned a risk ranking. This part of the assessment could be broken into categories such as ATM/Debit Card Services, Share Products, Loan Products, Credit Cards, Electronic Banking Services, Monetary Instruments, Wire Transfer Services, Safe Deposit Boxes, etc. In each area or category, consideration should be given to the types of transactions that can be conducted, the ease in which money can be moved from one account to another, the dollar amounts of the transactions, and the geographic location of the beneficiary of the transaction. Non-member transactions should also be considered; for example, nonmembers cashing “on us” checks; nonmembers signing as cosigners or guarantors on a loan; nonmember cash advances; nonmembers as account beneficiaries or signers on safe deposit boxes, etc. Again, once a risk ranking has been assigned, current procedures for each product and service should be analyzed to determine if extra due diligence is required for transactions identified as high risk or if ongoing monitoring for suspicious activity is necessary.



Continued from page 2

**Member Information Risk Assessment**

As part of each credit union's information security program, NCUA Regulation 748 requires credit unions to assess the risk to member information and member information systems to identify "reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction" of that information or system. Member information systems are defined as "any method used to access, collect, store, use, transmit, protect, or dispose of member information."

An initial risk assessment serves as a baseline for credit union initiatives and for forming a basis for determining how the risks should be managed to an acceptable level. The process should provide for risk assessment at both the global level and system specific level. Reassessments should occur periodically whenever new products, services, and vendors are added or when existing systems or vendors are changed. The risk assessment provides a point to refer back to when making modifications to existing systems to determine if a modification will require a change to existing controls. The risk assessment information should also be updated with results of audits, inspections, and identified incidents.

The risk assessment should encompass electronic, physical, and verbal risks to member information and member information systems. Obviously the scale and complexity of a credit union's operations and the nature of products and services offered will determine what threats may exist for that credit union. The risk assessment should identify the threats, their probability of occurrence, and the potential impact on the Credit Union if the threat did occur. Then Management should determine what, if any, safeguards or internal controls are currently in place to reduce the risk of the threat from occurring, as well as the adequacy of those safeguards or controls. The table below outlines an example of an electronic, physical, and verbal risk to member information:

System	Threat	Probability L=Low M=Medium H=High	Potential Impact L=Low M=Medium H=High	Safeguards/Internal Controls
Data stored on servers	Electronic: A virus, or malware application, if able to deploy on the system could destroy, corrupt, or disclose data to unauthorized parties.	M	H Possible economic loss, data integrity and confidentiality loss, reputation loss	1. Enterprise level anti-virus software employed with automatic updates 2. External drives limited to specific employees 3. Network policy in place 4. Employees must acknowledge reading the Internet Acceptable Use policy 5. Periodic training on Internet and email use
Data stored in paper format	Physical: Unauthorized physical access to files or documents containing confidential member information	L	H Possible economic loss, data integrity and confidentiality loss, reputation loss	1. Monitored alarm system to the building 2. Badge entry key card access system with restricted access based on job function 3. Video cameras monitor certain sensitive areas 4. Receptionist at front door 5. Visitors required to sign log 6. Visitors escorted in restricted areas
Data given over the telephone	Verbal: Sensitive or confidential information may be given verbally to unauthorized persons	L	M Possible economic loss, data integrity and confidentiality loss, reputation loss	1. Confidentiality agreement signed by all employees 2. New hire orientation training covers confidentiality 3. Annual policy review covers confidentiality 4. Telephone procedures prohibit giving account or social security numbers 5. Telephone member identity verification procedures in place

Continued on page 4

*Continued from page 3*

Once the threats and safeguards to mitigate those threats have been identified, the safeguards and internal controls should be tested. Testing will help determine the adequacy of the safeguards and how effectively they are working to mitigate the credit union's risks. Additional controls or changes to current procedures may be identified during the testing, and the results of the testing should be used to update the documented risk assessment.

**Disaster Recovery/Business Continuity Planning**

NCUA Letter 01-CU-21, "Disaster Recovery and Business Contingency Plans" and the FIEC IT Booklet, "Business Continuity Handbook" outline the steps necessary to developing a comprehensive plan that covers the entire credit union's operations rather than just information systems or data processing operations. The first step in developing a plan is to conduct a business impact analysis. The business impact analysis identifies all of the critical systems, products, and services at the credit union and establishes minimum allowable downtime for each critical service along with personnel, equipment, vendors, etc. necessary to conduct that service. The business impact analysis helps to prioritize recovery of critical services.

The second step in developing a plan, and the one we will focus on here, is conducting a risk assessment. A risk assessment, for disaster recovery planning purposes, identifies threat or failure scenarios that may possibly disrupt the credit union's business operations; taking into consideration the probability of occurrence and the potential impact of the occurrence. Some failure scenarios will require little action on the part of the credit union, while other scenarios will require detailed contingency plans.

Threat or failure scenarios identified should be comprehensive and take into consideration some of the following (this list is not all inclusive):

- ▶ Natural Threats
  - Natural disasters such as hurricanes, tornadoes, floods,

- blizzards, electrical storms, and earthquakes.
- External threats such as fire, power outages, chemical spill, and wind damage from falling trees.
- Pandemic threats such as the bird flu or SARs
- ▶ Technical Threats
  - Failure of system hardware/software
  - Failure or malfunction of servers/PBX
  - Loss of communication lines
  - Power brown outs or fluctuations
  - Loss of physical access to resources
  - Power failure in select areas
  - Heating, ventilation, or air-conditioning failure
  - Failure of backup tapes
- ▶ Human Threats
  - Bomb threat
  - Burglary
  - Civil disorder
  - Improper handling of sensitive data
  - Unauthorized access to sensitive data
  - Intentional data error entry
  - Loss of key position/management personnel
  - Loss of key members to respond to a disaster
  - Kidnapping
  - Malicious damage to equipment
  - Riots
  - Sabotage
  - Theft
  - Unauthorized modification to software
  - Unauthorized physical access to the premises
- ▶ Internal Disasters
  - Electrical fire
  - Water flooding or leakage
  - Loss of backup power systems
  - Heating, ventilation, or air-conditioning failure
  - Loss of physical access to resources
  - Loss of access to vital records
- ▶ Third Party Service Providers
  - Failure of third party service provider as a going concern

- Multiple disasters occur putting a strain on third party services
- Disaster at the third party site
- Unauthorized access to member information at the third party location

The threats and failure scenarios should be rated as to the probability of occurrence, the warning time that might be given prior to a disaster, and the impact the threat would have on the credit union. Mitigating controls should also be considered in the risk ranking; for example, if the credit union has a monitored fire alarm system in place that might reduce the risk of an internal fire from doing much damage. The risk assessment should include all of the credit union's locations and facilities in order to ensure a comprehensive plan is developed.

**“Credit unions are expected to perform a risk assessment and implement any changes to procedures and authentication methods by the end of 2006.”**

**E-Commerce Risk Assessment**

In November 2005, NCUA published Letter 05-CU-18, "Guidance on Authentication in an Internet Banking Environment." This letter calls on credit unions to assess the risk in their e-commerce environment to determine whether current member authentication methods for e-commerce activities are adequate for the volume and complexity of transactions conducted using these systems. Authentication is a tool to help prevent unauthorized access to member information, fraud, and identity theft. Credit unions are expected to perform a risk assessment and implement any changes to procedures and authentication methods by the end of 2006.

Authentication is the process of verifying a member's identity prior to the member gaining access to the Internet banking system.

*Continued on page 5*

*Continued from page 4*

Many systems currently use an authentication method known as “single factor” authentication. Single factor authentication methods typically use something the user “knows” such as a password or PIN in conjunction with an identity reference or user name. Authentication methods that use more than one factor are more difficult to compromise than single factors. Multi-factor authentication methods usually consist of a combination of some piece of information the user knows plus something in the user's possession. For example, an ATM card and PIN are considered a multi-factor authentication method, as to get money from the ATM, it requires two items: something the user has (an ATM card) and something the user knows (the PIN). Other multi-factor authentication methods include the use of other tokens (such as smart cards, USB tokens, etc.), biometrics, Internet Protocol Address and Geo-location, and digital certificates and mutual authentication. Shared secrets, whereby the member must answer a series of challenge questions or select a predefined image when logging on, would be considered a layering security technique when used in combination with the user name and password, as this would also be “something the user knows.” (See the FFIEC enclosure to Letter 05-CU-18 for a more detailed discussion on the various multi-factor authentication methods.)

Depending on the types of activities available or allowed through e-commerce systems, the FFIEC and other regulatory bodies have determined that single factor authentication methods may not be adequate to protect member information; hence, the need to conduct a risk assessment in this area. In conducting the risk assessment, consideration should be given to the types of transactions allowed, the dollar amount of transactions, the ease in which money can be transferred from one account to another, volume of transactions, type of member involved (individual vs. business), and the sensitivity of member information being communicated through the system. Some questions to pose during this risk assessment:

- ▶ What types of transactions are allowed through the home banking application?
  - Can members request checks be sent to their home address of record?
  - Can members change their address through the home banking application?
  - Can members transfer funds to (push) another member's account?
  - Can members transfer funds from (pull) another member's account?
    - Does the member have to be a joint signer on the account or can the member transfer money to or from another's account without being a joint signer?
  - Is there a dollar limit to the amount that can be transferred in any one transaction?
    - During any one time-frame?
- ▶ What types of transactions are allowed through the bill payment application?
  - Can members “pay” an individual as well as a business account?
    - Is an account number required to process the transaction?
  - Is there a dollar limit to the amount that can be paid in any one transaction?
    - During any one time-frame?
- ▶ Are electronic wire transfers allowed through any of the e-commerce applications?
  - Do the types of wires include international wires?
  - Must the member be the beneficiary of the money at another institution or can the money be wired to a third party?
- ▶ Can prospective members sign up online for membership at the credit union?
- ▶ Can members open new accounts through any of the Internet Banking applications?
- ▶ How strong are current authentication methods?
  - Are password parameters set at a minimum of 8 alphanumeric characters?
  - Must members change their passwords after a set cycle (30 days, 60 days)?
  - Are members forced to change their password upon initial logon?
  - Is the member's social security number used for any part of the user name and/or password?
  - Are logon attempts restricted to three and then the account is locked out?
  - Is the application set to automatically log off after a set period of inactivity (i.e. 10 minutes)?
  - Does the application track the member's IP address, and if different, implement a set of security questions?
  - What type of education does the credit union give the member related to Internet and email frauds and schemes?
  - What type of monitoring is in place over e-commerce activities to monitor for suspicious activity?

**“The types of e-commerce activities offered will play a large role in determining the risk the credit union faces.”**

These are just some of the questions Management should consider when conducting this risk assessment. The types of e-commerce activities offered will play a large role in determining the risk the credit union faces. Then each activity should be analyzed as to what procedures and processes are in place at your individual credit union in order to determine whether current authentication methods are adequate or could be strengthened by multi-factor authentication methods, security layering techniques, or other controls to reasonably mitigate the risks identified.

*Continued on page 6*

**In This Issue:**

**Accounting  
& Auditing 1**

**Risk  
Assessment 2**

**Did You  
Know 6**

**RISK ASSESSMENT CON'T.**

*Continued from page 5*

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Existence of risk is not, by itself, a reason for concern. Rather, Management must consider whether the risks are warranted. Risks are warranted if they are understandable, controllable, and within your Credit Union's capacity to readily withstand adverse performance. A risk assessment in each of these areas will help Management, the Board of Directors, and the Supervisory Committee understand each area's risks and determine whether sufficient controls are in place to reduce the risk to an acceptable level.

*Rachel Fisher, CISA, NCCO  
Partner*



To hear more on these "hot button" issues, plan to attend AICPA's National Conference on Credit Unions, October 25-27, 2006 in Orlando, FL. The AICPA National Conference on Credit Unions is packed with critical training on all the latest changes impacting Credit Unions and their auditors.

Be sure to catch our Associate, Rachel Fisher's session on the BSA/OFAC/Patriot Act. Rachel's session will cover the Bank Secrecy Act and other AML regulatory deficiencies. It will also cover these important areas: Basic requirements, common violations/deficiencies, risk assessment, monitoring, and transaction testing.

Don't miss this stimulating and informative conference. We look forward to seeing you there!

**ABOUT US**

**Nearman ♦ Maynard ♦ Vallez**

CPAs & Consultants, P.A.

Nearman, Maynard, Vallez, CPAs & Consultants, P.A. provides audit and consulting services to credit unions across the United States. If your Supervisory/Audit Committee or Management is interested in obtaining information on the subjects in this issue or about our services, call the firm that has specialized in the credit union industry since 1979.

Website: [www.nearman.com](http://www.nearman.com)  
E-mail: [info@nearman.com](mailto:info@nearman.com)  
Toll-free: (800) 288-0293

Direct to one of our offices:  
**Atlanta:** (770) 461-5706 FAX (770) 719-1888. Ask for Rachel Fisher.

**Miami:** (305) 598-1730 FAX (305) 595-9316. Ask for Cecil Maynard, Chris Vallez, or Jennifer Hoskins.

This newsletter is for information purposes only and is not intended to provide investment, legal or accounting advice. Edited by Rachel Fisher, CISA, NCCO, Partner. No part of this newsletter may be reproduced without the written consent of Nearman, Maynard, Vallez, CPAs & Consultants, P.A.