

Corporate Network Information Security Risk Management Framework

**Version 1.1
Date: April 27, 2006**

Table of Contents

Table of Contents	i
Document Record.....	ii
Association of Corporate Credit Unions Disclaimer.....	iii
Introduction.....	1
Background.....	1
Objectives.....	2
Approach	3
Regulatory Guidance	3
Administration & Planning Guide	5
Program Administration/Project Planning.....	5
Roles and Responsibilities:.....	5
Choosing a Methodology	7
Outsourcing Your Risk Assessment	7
Policies and Procedures.....	7
Risk Assessment Triggers:	8
Vendors/Service Providers:	8
Key Elements.....	9
Purpose	9
Organizational vs. Application Risk Assessments	9
Step 1. Business Process Identification	11
Step 2. Prioritization	12
Step 3. Asset Identification.....	13
Step 4. Threat Identification	14
Step 5. Identify Control Requirements.....	15
Step 6. Identify Vulnerabilities.....	16
Step 7. Risk Determination.....	18
Step 8. Develop Risk Mitigation Strategies.....	19
Step 9. Residual Risk Identification	20
Step 10. Risk Monitoring and Reporting.....	21
Information Security Risk Management Maturity Model.....	22
Maturity Model.....	22
Purpose	22
CMM Matrix	33
Reference Materials	37
Terminology	37
NIST Risk Assessment Methodology.....	39
OCTAVE Risk Assessment Methodology	40
Appendix A (Business Processes)	41
Appendix B (Asset Listing)	42
Appendix C (Threat Listing)	43
Appendix D (Vendor Listing)	49

Document Record

Revision History

Revision Date	Version Number	Revision Description	Author of Revision
2/01/06	1.0	Final	Jean Golka- ISRA Workgroup
4/27/06	1.1	ACCU Disclaimer	Rhonda Whitley-ACCU

Association of Corporate Credit Unions Disclaimer

The information contained in this document was developed by the Corporate Network for use by corporate credit unions, and the authors of this document assume no responsibility beyond its intended use. Some or all of the contents of this document may not be applicable to natural person credit unions and in no way constitutes legal advice. Please consult your own advisors for guidance on specific compliance matters.

Introduction

Background

In recent years there has been an increase in the number of attacks against financial institutions' information systems and networks. This requires management of the risks posed by a wide range of potential attackers, including disgruntled workers, mischievous employees, industrial spies and hackers. Information security risk assessment is the process used to identify, understand the risks to confidentiality, integrity and availability of information and information systems. Information security risk management is the process used to mitigate and continuously monitor assets for emerging risks.

As a result, it was recommended that a Corporate Network information security risk review team be assembled to analyze industry guidance and best practices, identify Corporate Network collaborative opportunities, and work cooperatively with the NCUA to reach a common understanding of expectations and standards around information security risk management practices. The Workgroup participants include:

ACCU:	Mike Canning, Executive Director Rhonda Whitley, Compliance Manager
Empire Corporate:	Chris Duwe, Assistant Vice President, Operational Integrity Kristine Cottom, VP, Information Systems
Iowa Corporate:	Jeff Russell, CIO / Vice President, Strategic Development
Mid-States Corporate:	Ed Brooks, Vice President, Information Systems
Southeast Corporate:	Brian Avril, Sr. Vice President / CFO – Finance Greg Moser, Business Systems Project Manager Karen Gispanski, Network Security Administrator Barry Haddix, VP / Information Technology – Information Systems
Southwest Corporate:	Jerry Delezen, IT Director Justin Lutes, Business Continuity and Operations Compliance Manager
U.S. Central:	Sandi Brady, Vice President, Internal Audit & Compliance Tony Ferris, Vice President, Member Services Jean Golka, IT Risk Manager Chris Hyers, Director IT Security Cliff Rippe, IS Business/Compliance Manager Pam Whiteley, Project Assistant, Business/Compliance
WesCorp:	Gene Berger, Vice President of Information Technology

Objectives

- 1. Objective: Work cooperatively with the Corporate Network and NCUA to establish a reasonable and effective framework for information security risk management (i.e. risk assessments, risk mitigation planning, and testing and re-evaluation practices).**

A Workgroup was established that included a cross-section of personnel from the Corporate Network. Utilizing conference calls and workshops, the Workgroup strived to establish a common framework around information security risk management practices and shape corporate regulatory guidance. The first task was to review criteria provided by the Federal Financial Institutions Examination Council (FFIEC) and National Credit Union Administration (NCUA) on information security risk assessments. An evaluation of a number of industry accepted methodologies (i.e. NIST, Octave, Octave-S, etc.) was then completed to identify those components that were consistent in each methodology. Finally, based on this information, the Workgroup developed a generic overview of an information security risk management process, including details about each component and examples. In addition, efforts were made to receive clarification on definitions and deliverables from the NCUA.

- 2. Objective: Facilitate education and information sharing around information security risk management practices.**

The Workgroup will work to identify opportunities to identify, promote and provide in-depth training on information security risk management best practices. This may also include leveraging third party vendors that provide training on industry accepted information security risk assessment methodologies.

- 3. Objective: Explore collaborative opportunities within the Corporate Network to reduce expenses and enhance capabilities around information security risk management practices.**

The Workgroup identified collaborative opportunities such as combined due diligence efforts for third party vendors, knowledge sharing and combined training efforts provide an opportunity to reduce expenses and enhance capabilities. *As of the published date, a corporate workgroup led by Corporate One Federal Credit Union is forming to perform a risk assessment of the Fedline Advantage system.*

- 4. Objective: Establish best practices for the assessment of third party systems and the establishment of member assessment responsibilities.**

Risk assessments are required on all systems regardless of whether those systems reside in-house or with a third-party. Additionally, as a supplier of outsourced services, the Corporate Network has obligations to provide due diligence to its customers surrounding the safety and soundness of their systems and confidential data as a component of their fiduciary responsibilities. For example, natural person credit unions rely on their corporate partner and the corporates rely on U.S. Central to provide evidence of the safety and soundness of their systems and data. *The workgroup will work with the Vendor Management workgroup and Fedline Advantage pilot group to better articulate best practices around working with third parties. In addition, the workgroup will work to develop a consensus regarding the type*

information provided by the Corporate Network to its members regarding its information security risk management practices. This information will be provided in subsequent updates to this document.

Approach

This effort is intended to establish a common framework of best practices around information security risk management practices, explore collaborative opportunities to enhance operations and/or reduce expenses, and cooperatively shape compliance expectations.

While the Corporate Network Information Security Risk Management Framework provides for a common understanding of information security risk management across the Corporate Network, it is understood that the quality and maturity of corporates' current information security risk management programs, as well as their future programs, will vary. As such, the proposed approach to be taken by each corporate in implementing the Corporate Network Information Security Risk Management Framework centers around the following steps:

- Determine the maturity of the current Information Security Risk Management program based on the "characteristics" within the Maturity Model.
- Complete a gap analysis of current Information Security Risk Management program to desired maturity level.
- Using the guidelines in this document, develop a plan and timeline for completing the specific tasks and deliverables necessary to achieve the desired maturity level.
- Reassess quality and maturity of Information security risk management program (ongoing).

Recognizing the complexity of each corporate's business activities, as well as the variances in size of staff, the Workgroup believes the proposed information security risk management framework to be scalable for all corporates. For example, the Maturity Model identifies specific criteria to be met to achieve levels within the model. While each of the criteria, task and deliverables may not be reasonable or achievable for all corporates, an evaluation of such, with documented analysis of the outcome, provides a basis for common understanding within the corporate, as well as external constituents (e.g., regulators, auditors, etc.)

Minimum Recommended Maturity Level

The workgroup is in agreement that the minimum level of maturity a corporate should achieve is Level 3 – Defined. The time horizon for achieving this goal is dependent upon the corporate, as each institution is unique. The corporate should ensure that they have taken adequate time to fully understand the need for sound risk management program and has developed a reasonable and comprehensive plan to reach the desired level of maturity.

Regulatory Guidance

The published regulatory guidance on information system risk management is noted below with corresponding web links.

The NCUA issued the Corporate Credit Union Guidance Letter 2004-03, Critical Information System Risk Areas on August 9, 2004. The guidance addresses the corporate credit union's responsibilities for performing information security risk assessments.

[NCUA Corporate Credit Union Guidance Letter 2004-03](#)

The Federal Financial Institutions Examination Council (FFIEC) issued the FFIEC Information Technology Handbook on Information Security in August 2003. The handbook includes guidance on performing information security risk assessments. The FFIEC has issued ten Information Technology Examination Handbooks on various topics relevant to Corporate Network information technology systems. The handbooks can be useful in establishing mitigating controls.

[FFIEC Information Technology Examination Handbooks](#)

The FFIEC IT Examination Handbook on Information Security states, in part, that as part of its risk management process, each corporate should have:

1. Characterized and prioritized their business processes/assets; according to a consistent methodology that considers the risks to customer non-public information as well as the risks to the institution.
2. Identified all reasonable threats to the institution (with consideration for emerging threats).
3. Analyzed its technical and organizational vulnerabilities.
4. Considered the potential effect of the security breach on customers as well as the institution.
5. Ensured that the risk assessment provides support for the corporate's security strategy, controls and testing plan.

Further, in order to be effective, the risk management process should incorporate the following practices:

- Multidisciplinary and knowledge-based approach
- Systematic and centrally controlled
- Integrated process
- Accountable activities
- Documented
- Knowledge enhancing
- Regularly updated

Finally, the institution should effectively update the risk assessment when confronted with any new conditions that would affect the risk analysis, including changes to assets, threats and vulnerabilities. Absent of any changes, the organization risk assessment should be revisited at least once a year to verify asset criticality and risk assessment plans.

Administration & Planning Guide

Program Administration/Project Planning

Key elements of a risk management plan:

- Formal designation of responsibilities across the organization for the risk management capability
- Selection, training and utilization of an industry-proven methodology
- Commitment to following the key principles of the FFIEC
- Establishment of time frames for piloting and implementing a risk management capability

Roles and Responsibilities:

Information security is the joint responsibility of everyone at the financial institution including service providers and contractors. While each corporate's organizational structure will dictate the actual assignment of responsibilities; a list of potential roles is provided below:

Employees/Contractors – Accountable for filling their security responsibilities as defined in the security policy and job descriptions or contracts

Business/Product Owner – owner of business process/product – Maintains ownership of and is a major participant in the information security risk management process

Subject Matter Experts – Participants with resident knowledge of the organization, specific applications or processes as required in the risk management process

Security Officer – Facilitates the information security risk assessment process

Risk Committee – optional role driven by complexity of the organization – Determines level of acceptable risk according to parameters provided by the board of directors

Senior Management – Final reviewers of the risk assessment documentation prior to submission to the risk committee or board of directors; responsible for oversight of the information security risk management program, including risk assessments, risk mitigation strategies and risk acceptance

Board of Directors – Ultimate responsibility for the governance of the corporate information security program and acceptance of the level of risk to the organization; responsible for establishing risk acceptance expectations (thresholds)

External/Internal Audit – Evaluates the information security risk management process and deliverables in light of regulatory guidance and industry standards

Choosing a Methodology

It is recommended that the institution choose an established methodology for performing information security risk assessments and/or ensure that employees responsible for performing the same receive appropriate training. The NCUA Corporate Credit Union Guidance Letter 2004-03, Critical Information System Risk Areas, identifies three which may be helpful. These are the most common methodologies in use in the corporate network.

- NIST SP 800-30, Risk Management Guide for Information Technology Systems
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- OCTAVE Framework, Version 2.0
<http://www.sei.cmu.edu/pub/documents/01.reports/pdf/01tr016.pdf>
- OCTAVE-S Framework, Version 1.0 (for small organizations)
<http://www.sei.cmu.edu/publications/documents/04.reports/04hb003.html>

The three frameworks follow the same basic principles identifying assets, threats, vulnerabilities to identify and analyze risks in order to develop protection strategies and mitigation plans; with the ultimate goal to help organizations better manage information security risks. The OCTAVE frameworks are more structured, providing templates and surveys to help guide an organization through the risk management process. The NIST framework provides the outline for performing risk assessments, but allows an organization additional flexibility in tailoring each step in the process. Both are considered industry-proven methods for risk management and can and should be customized by each corporate to meet its particular needs, especially in relation to GLBA compliance. However, corporates should remain cognizant that any changes made do not invalidate the underlying methodology.

Outsourcing Your Risk Assessment

The corporate may choose to leverage external expertise in conducting information security risk assessments until a transfer of knowledge occurs to parties within the corporate. Selection of a third party vendor should be approached cautiously to ensure that the guidelines established by the FFIEC have truly been incorporated into the methodology adopted and deliverables to be provided. Choosing a third-party vendor to help the corporate through an initial risk assessment has been found to be beneficial, but it does not absolve the corporate of taking ownership of the risk management process and developing a full understanding of the risk management process.

Policies and Procedures

It is recommended that the following components be addressed through your organization's board policies:

- Description of the information security risk management process at both the organizational level and business process/ application level
- Guidelines for establishing priorities in conducting the information security risk assessments
- Identified "triggers" that would require an update to an existing information security risk assessment

- Assigned decision rights for the acceptance of security risks
- Requirements for management reporting, consistent with the corporate's management reporting and organizational structure

Risk Assessment Triggers:

Risk assessments should be updated as new information affecting risks are identified or within specified timeframes. Significant changes should trigger a revisit of the risk assessment. The determination of key events is subjective; thus each corporate must make its own determination as to what constitutes a significant event. It is acceptable to only revisit the portion of the risk assessment that addresses the elements subjected by the change and the elements affected by those changed elements, not necessarily the entire assessment. Examples of significant events may include the following:

- Large scale system changes; upgrades
- Additional software modules
- Significant software releases
- Emerging threats and vulnerabilities
- Significant vulnerabilities identified in the normal course of business

Vendors/Service Providers:

Each corporate is required to perform an information security risk assessment on those products or services supported by an outsourced service provider. This would include products/services provided by U.S. Central to the corporate network; those provided by a corporate to a natural person credit union, or those provided by a third-party to any of the above. In all cases, the corporate is responsible for completing the necessary due diligence to ensure the safety and soundness of the product/service being outsourced; this includes identifying and managing the risk environment.

This framework will be utilized for a Corporate Network risk assessment of Fedline Advantage As a result of that assessment and in conjunction with the Corporate Network Workgroup on Vendor Management, the workgroup will develop and publish additional guidelines for performing risk assessments of vendors and service providers.

Key Elements

Purpose

Financial institutions have become increasingly reliant on information technology to deliver financial services to their customers. Further, the advances in technology have necessitated such regulations such as the Gramm-Leach-Bliley Act (GLBA) that impose stringent requirements upon financial institutions to safeguard non-public information. Both of these have resulted in changes to a financial institution's traditional risk environment. While the financial institution's primary operational/transaction risks from fraud, theft or accidental damage remain, this increased reliance on technology has resulted in an environment in which the number and nature of potential threats and vulnerabilities to a financial institution and its non-public personal information are in a constant state of flux.

Therefore, the corporate must implement a pro-active risk management program to address the dynamic risk environment. The primary purpose of information security risk management is to ensure board and management awareness of risks posed to information assets, particularly risks to consumer non-public personal information, and to allow board and management to develop appropriate policies and procedures to pro-actively manage these risks. The risk assessment should provide the basis for the organization's information security program and testing plans and is a primary input into the information security strategic planning process.

Organizational vs. Application Risk Assessments

Information security risk assessments should be performed at two levels: organization-wide and application or system specific, as appropriate. Both types of assessments should utilize the same methodology, including all of the key elements identified below, but at different levels of granularity. While the workgroup recommends starting with the organizational risk assessment, there is no right answer as to which to perform first. There are benefits to performing an application risk assessment first to test the risk management program before performing an organizational assessment.

Organizational Information Security Risk Assessment – When getting started, the corporate should identify and group all business process and, if applicable, information assets for analysis of criticality. Logically grouping like assets by functionality (internet routers), application or system (wire system) is recommended. The criticality rankings then guide the performance of individual application/system risk assessments. As each application risk assessment is performed; the results should contribute to the organizational assessment.

In addition, as part of the organizational risk assessment; management should identify those practices (i.e. physical security; HR practices) that are consistent across the organization. These should not need to be reassessed for each application, but instead could be addressed once, for the organization as a whole.

Application Information Security Risk Assessment – An application information security risk assessment focuses on the discrete application/system involved in a business process with established boundaries. The application information security risk assessment typically involves significantly more detailed analysis than an organizational information systems risk assessment. Such assessments should be performed on both existing and new applications. The risk assessment should be incorporated into the corporate's acquisition and development processes. As noted above, these assessments then become a subset of the organizational information risk assessment.

Step 1. Business Process Identification

To begin, management needs to understand the business critical assets that are in need of protection. Thus, the security risk assessment, like the business continuity risk assessment, should begin with the identification of business processes.

Key Principles (FFIEC Guidance)	Financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories.
Thought Criteria	This step is recommended as the starting place for the organization's assessment process, whether using OCTAVE or NIST as the risk assessment methodology. Identifying business processes will help management pinpoint key areas in which to start the information security risk assessment process.
Information Gathering	Business Continuity Business Impact Analysis (BIA) Note: The first step in performing the Business Continuity BIA is determining the key business processes of the organization. If the organization has not yet started the BIA, this exercise will be beneficial for both the BIA and the security risk assessment.
Activities	Identify all processes that support the business through questionnaires, interviews, existing documentation, etc.
Suggested Output	List all business processes.
OCTAVE	Phase 1 – Build Asset Based Threat Profiles
NIST	Step 1 - System Characterization

Step 2. Prioritization	
The next step is to rank the business processes identified in importance to the institution to determine an overall risk management plan.	
Key Principles (FFIEC Guidance)	Financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories.
Thought Criteria	<ul style="list-style-type: none"> • The ranking of business processes in the Business Continuity BIA is focused on the availability of systems. For ranking business processes as part of the information security risk assessment, the ranking of such systems is dependent on the sensitivity of the information processed. • The existence of non-public, personal information (per GLBA) should necessitate a high criticality ranking. • Business process criticality should also consider protective needs regarding confidentiality, integrity, and availability. • The following criticality definitions are provided as an example: <ul style="list-style-type: none"> ○ Critical – the compromise of the information or process would be catastrophic to business operations ○ High – the compromise of the information or process could be critical to business operations ○ Medium – the compromise of the information could result in degraded business operations ○ Low – the compromise of the information would have negligible effects on business operations
Information Gathering	Business Continuity BIA Business Process Listing
Suggested Activities	Analyze all business processes and rank them according to the sensitivity of information processed, especially GLBA data and the criticality to business. <i>For example: A system that is utilized in the purchase of natural person loans may not be critical to the corporate as far as the dollar volume contribution to net/gross income and/or asset size; but the data stored to support the sale of the loans could be considered critical for information security purposes in that it can contain non-public personal information per GLBA, which could result in significant loss to the institution if compromised.</i>
Suggested Output	List primary business processes, ranked in importance regarding the criticality to operations, as well as the sensitivity of data stored on the system.
OCTAVE	Phase 1 – Build Asset Based Threat Profiles
NIST	Step 1 -System Characterization

Step 3. Asset Identification	
The next step in the information security risk assessment process is to identify the specific assets to be assessed.	
Key Principles (FFIEC Guidance)	Articulate understanding of the system, including the boundaries of the system being assessed, the system's hardware and software, and the information that is being stored, processed and transmitted.
Information Gathering	<ul style="list-style-type: none"> • Existing inventories from asset management database • Include information, systems, services and applications and people • Include the physical location/building
Thought Criteria	<ul style="list-style-type: none"> • Driven by the business process • Consider both manual (i.e. transport and storage of backup tapes) and automated processes • Personnel can be grouped in various categories depending upon the organization structure of the organization. • Assets may be shared by several business processes or unique to a specific business process; consider identifying assets as organizational-wide (email) or specific to a business process • Consider grouping of like assets by functionality • Consider the sensitivity of data regarding GLBA, HIIPPA, etc. • Consider potential harm to customers of unauthorized access and disclosure of non-public personal information
Suggested Activities	<ul style="list-style-type: none"> • For each business process, identify the physical, logical and human resources that support that process • Identify the type of data that is being stored, processed and transmitted • Group like assets by functionality as appropriate (i.e. internet routers) • Determine the boundaries for each asset grouping (i.e. core processing, wire transfer systems, etc.) • Designate each asset as specific to the application or shared by the organization
Suggested Output	Asset listing designated to a specific group or organization-wide
OCTAVE	Phase 1 – Build Asset Based Threat Profiles
NIST	Step 1 – System Characterization

Step 4. Threat Identification

Once management has identified the assets included in the assessment, the next step is to perform a threat analysis. The analysis helps management to identify the potential threats that could potentially harm or disrupt those assets as identified.

Key Principles (FFIEC Guidance)	Threats are identified and measured through the creation and analysis of threat scenarios. Scenarios should include attacks against the logical security, physical security and combinations of logical and physical security.
Information Gathering	<ul style="list-style-type: none"> • Threat databases exist, an example is included in the Appendix • Sources for ongoing monitoring of emerging threats (security websites; magazines, etc.)
Thought Criteria	<ul style="list-style-type: none"> • Identification of a threat (e.g. hacker) must also include the threat action (e.g. worm) • A threat is an activity that potentially could harm or disrupt a computer system, software application or other operation • Threats may bring harm through: <ul style="list-style-type: none"> ○ Destruction – the loss of the asset ○ Disclosure - the divulgence of confidential information ○ Modification – the compromise of data or system integrity ○ Denial of Service – the loss of use of the asset • Threats can be accidental (non-malicious), intentional (malicious) or environmental (natural)
Suggested Activities	<ul style="list-style-type: none"> • Identify the threat scenarios unique to the corporate, including the threat actions • Research and monitor emerging threats • Link potential threats to the assets that may be vulnerable to these threats (specific to the scope of the assessment)
Suggested Output	Threat Matrix/Profiles <i>Note: Management should maintain a master Threat Matrix for use in risk assessments. The Threat Matrix should then be tailored for the specific system/organization under review.</i>
OCTAVE	Phase 1 – Build Asset Based Threat Profiles
NIST	Step 2 – Threat Identification

Step 5. Identify Control Requirements

Risk consists of a threat and vulnerability pair. To determine the risk to the organization, management must identify potential control requirements as well as existing controls already in place to protect against potential threats.

Key Principles (FFIEC Guidance)	Identify security requirements and considerations. Document current controls and security processes, including both logical and physical security.
Information Gathering	Gather control requirements from: Industry Best Practices Regulatory Guidance Gather key control information through: <ul style="list-style-type: none"> • Surveys • Internal procedures • SAS No. 70 Reviews • Agreed-upon-procedures Reviews
Thought Criteria	<ul style="list-style-type: none"> • Manual and/or automated controls may already exist to assist management in its assessment.
Suggested Activities	<ul style="list-style-type: none"> • Starting with the asset/asset grouping identified and the threat scenarios developed, management should: <ul style="list-style-type: none"> ○ Develop a Security Requirements Checklist <ul style="list-style-type: none"> ▪ Industry Best Practices ▪ Regulatory Guidance ○ Document current security controls ○ Identify testing used to provide assurance that control works as designed and is efficient and effective • Testing of controls: <ul style="list-style-type: none"> ○ Pre-Implementation – testing/verification of controls can be performed by project team ○ Post-Implementation – testing/verification of controls should be performed by an independent party
Suggested Output	Security Requirements Checklist Existing Controls
OCTAVE	Phase 1 – Build Asset Based Threat Profiles
NIST	Step 4 – Control Analysis

Step 6. Identify Vulnerabilities

Risk consists of a threat and vulnerability pair. Areas in which such controls are not adequate to protect against the threat are identified as vulnerabilities.

Key Principles (FFIEC Guidance)	Identify security requirements and considerations. Identify organizational vulnerabilities (weak management support, ineffective training, inadequate policies and procedures). Identify technical vulnerabilities (hardware and software configurations).
Information Gathering	Gather key vulnerability information through: <ul style="list-style-type: none"> • Internal Audits • Penetration Tests • Vulnerability Tests/Scans • SAS No. 70 Reviews • Agreed-upon-procedures Reviews • Code Reviews • Surveys/Questionnaires • Security Requirements Checklist <ul style="list-style-type: none"> ○ Regulatory Guidance ○ Information Security Best Practices ○ Vulnerability Notification Services (Microsoft, UNIX, etc.) ○ Information Security periodicals, websites, newsbytes, etc.
Thought Criteria	<ul style="list-style-type: none"> • Utilize information already available to the organization to determine compliance with the Security Requirements Checklist <ul style="list-style-type: none"> ○ Internal audits, penetration tests, vulnerability assessments, third-party reviews • Utilize surveys (as necessary) to determine compliance with Security Requirements Checklist • Testing for technical vulnerabilities can be internal or external to the organization • Leverage automated tests in conjunction with configuration reviews
Suggested Activities	<ul style="list-style-type: none"> • Starting with the asset listing and the threat scenarios developed, management should: <ul style="list-style-type: none"> ○ Use surveys/comparisons to best practices to identify gaps/vulnerabilities ○ Perform gap analysis with corporate information security program ○ Identify and perform technical analysis/testing as necessary ○ Identify gaps in controls/vulnerabilities ○ Identify asset/asset grouping on which the vulnerability exists • Determine if a viable threat scenario exists to exploit the vulnerability

	<ul style="list-style-type: none">• Analyze and rank each vulnerability identified
Suggested Output	Threat/Vulnerability pair, including ranking
OCTAVE	Phase 1 – Build Asset Based Threat Profiles Phase 2 – Identify Infrastructure Vulnerabilities
NIST	Step 3 – Vulnerability Identification

Step 7. Risk Determination

The goal of risk determination is to compile the information available and determine an asset's actual risk level. Risk determination combines the likelihood determination and impact.

Key Principles (FFIEC Guidance)	The risk from any given threat scenario is a function of the probability of the event occurring and the impact on the institution. The probability and impact are directly influenced by the financial institution's business profile, the effectiveness of the financial institution's controls and the relative strength of controls when compared to other industry targets.
Information Gathering	<ul style="list-style-type: none"> • Asset Listing • Threat Matrix • Testing/Survey documentation • Vulnerability listing • Compensating Controls
Thought Criteria	<ul style="list-style-type: none"> • Include all parties: business, information technology, and security personnel and third parties as necessary in risk determination process
Suggested Activities	<ul style="list-style-type: none"> • Identify the threat/vulnerability pair and asset affected • Rank the likelihood of the vulnerability being exercised by a threat; for example: <ul style="list-style-type: none"> ○ High – has the capability and motive to destroy or compromise an asset ○ Medium – has the capability to degrade asset's function ○ Low – has minimal capability or motive to harm asset ○ None – has no capability or motive • Rank the impact which would result from the successful threat exercise of the vulnerability; for example: <ul style="list-style-type: none"> ○ High – could allow the full control or destruction of the asset ○ Medium – could allow access to or compromise the asset ○ Low – could allow minor information gathering ○ None – no detectable issues • Assign risk level • Document analysis/thought process
Suggested Output	Prioritized lists of risks
OCTAVE	Phase 3 – Develop Security Strategy and Plans
NIST	Step 5 – Likelihood Determination Step 6 – Impact Analysis

Step 8. Develop Risk Mitigation Strategies

Once the risk determination is complete, management should identify additional controls necessary to mitigate the risk.

Key Principles (FFIEC Guidance)	A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of management action plans. Some risks do not meet the threshold established in the security requirement. Management can accept those risks and not proceed with a mitigation strategy. Other risks may require immediate corrective action. Still others may require mitigation over time.
Information Gathering	<ul style="list-style-type: none"> • Prioritized list of risks • Gather control information through: <ul style="list-style-type: none"> ○ Security Best Practices – NIST AP800-53, ISO 17799; COBIT ○ Corporate Information Security Program (Per Part 748 of NCUA Rules and Regulations) • Security Requirements Checklist
Thought Criteria	<ul style="list-style-type: none"> • Include all parties: business, information technology, and security personnel and third parties as necessary in risk determination process • Determine short-term and long-term solution
Activities	<ul style="list-style-type: none"> • Determine safeguards, timeline and affect on risk level in consideration of cost/benefit of additional safeguards • Assess if the risk can be reduced in the short-term vs. long-term • Determine impact of additional controls on risk level • Document analysis/thought process
Suggested Output	Recommended safeguards to be implemented.
OCTAVE	Phase 3 – Develop Security Strategy and Plans
NIST	Step 7 – Control Recommendation

Step 9. Residual Risk Identification

Once management has identified the risk level to the organization, management should attempt to identify the residual risk level for senior management and board personnel.

Key Principles (FFIEC Guidance)	Traditionally, management recognizes the direct impact on operational/transaction risk from incidents related to fraud, theft or accidental damage. Many security weaknesses can directly increase exposure in other risk areas, including legal/compliance risk, credit and market risk and reputation risk. An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities.
Information Gathering	<ul style="list-style-type: none"> • History of prior incidents • Current industry statistics • Business Impact Analysis • Business Operations Risk Assessment • Capital Plan • Insurance Policies
Thought Criteria	<ul style="list-style-type: none"> • Management should identify the residual risk to the institution • Generally, the residual risks which should be identified are those that management cannot substantially mitigate in the short-term. • Residual risk should be expressed in relation to the corporate as well as the member credit unions, if possible
Activities	<ul style="list-style-type: none"> • Determine impact of residual risk on business in relation to: <ul style="list-style-type: none"> ○ Reputation ○ Market Share ○ Revenues/Transaction • A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of management action plans. • Document value to the corporate for each identified risk
Suggested Outputs	Residual Risk Identification. Risk Assessment Report <ul style="list-style-type: none"> ○ Objectives and Scope ○ Summary of Critical Findings ○ Identification of Residual Risk
OCTAVE	NA (the framework does not address)
NIST	Step 9 - Results Documentation

Step 10. Risk Monitoring and Reporting

Once the corporate has completed the initial assessment, developed management action plans and identified residual risk, it is necessary to monitor management action plans and report on risk mitigation strategies.

Key Principles (FFIEC Guidance)	Documentation of risks accepted and risk mitigation decisions are fundamental to achieving accountability for risk decisions.
Information Gathering	Risk Assessment Report Management Action Plans
Thought Criteria	<ul style="list-style-type: none"> • Monitoring should be consistent with existing corporate reporting structures. • If mitigation strategies are not completed as scheduled, risk levels may actually increase. • If mitigation strategies are not well planned they may not be effective, thus increasing risk levels. • Changing circumstances may increase the residual risk beyond acceptable levels for acceptance and require additional measures.
Activities	<ul style="list-style-type: none"> • Develop a process for updating management progress, testing/validating controls (as needed). • Develop a reporting process to executive management and/or the Board. • Document management/Board acceptance of residual risk, as appropriate per risk management policy.
Suggested Outputs	<ul style="list-style-type: none"> • Progress Reports • Revised Risk Assessment Reports (as needed)
OCTAVE	NA (the framework does not address follow-up)
NIST	NA (the framework does not address follow-up)

Information Security Risk Management Maturity Model

Maturity Model

The Corporate Network Information Security Risk Management (CNISRM) maturity model developed by the workgroup is based upon similar models for information security and business continuity management and embraces the principle that the quality of the corporate information security risk management will be directly related to the quality and maturity of the information security risk management processes and practices used to create and maintain it. The CNISRM six level maturity model provides a step-by-step approach to improving information security risk management.

The principle behind maturity models is that an enterprise develops and adopts new processes and practices, from which it learns, optimizes and moves to the next level. There is a logical sequence to the steps; organizations can't skip a level – even if it moves through the stages at varying speeds. Such a model is a useful diagnostic tool – enterprises can use it to discern where it is and what it should do next. The model also serves as a prognostic tool to determine what is likely to happen next.

Purpose

The information security risk management maturity model helps Corporate Network members:

- Grade their information security risk management processes and practices
- Encourage senior management to appreciate what is required to improve the enterprise's risk management position
- Complete a gap analysis so that realistic targets can be set
- Provide a basis for peer-group comparison and establishment of industry standards

While corporates should strive to improve their information security risk management processes and practices, they shouldn't necessarily target "Level Five" as their goal. The effort to get to that stage may not be required to achieve a satisfactory level of risk mitigation for the corporate. **At a minimum, the corporate should achieve "Level Three" of the risk management process.**

The following is an overview of the model and the risk management program elements. A general set of characteristics for each level is presented as well as a matrix identifying the minimum criteria to achieve each level for each key element in the risk management process. Each of the minimum criteria must be met with supporting documentation for an organization to achieve a level.

Level 0 - Nonexistent

Characteristics:

- Information security risk assessments for processes and business decisions do not occur.
- The organization does not consider the business impacts associated with security vulnerabilities.
- Information security risk management has not been identified as relevant to acquiring IT solutions and delivering information technology services.
- Responsibilities and accountabilities for information security are not assigned.
- There is no understanding of the information security risks, vulnerabilities and threats to information technology/operations or the impact of loss of information technology/services to the business.

Key Element	Characteristics
Identify Business Processes	None
Prioritize Business Processes	None
Identify Assets	None
Identify Threats	None
Identify Vulnerabilities	None
Identify Existing Controls	None
Risk Determination	None
Develop Security Management Strategy	None
Residual Risk Identification	None
Risk Monitoring and Reporting	None

Level 1 - Initial

Characteristics:

- A loose or informal ISRA may have been performed, without following a defined process or standard.
- Informal assessments of information security risk take place at a functional or project level, without aligning to a standardized methodology or process.
- Findings may be identified, but no formal process exists to track or manage them.
- Some departments or functional areas with the organization may have taken some small steps, but there is no centralized approach or commitment.
- Assets, threats and vulnerabilities may be identified and documented informally, perhaps as part of the organizations disaster recovery plan or information security program.
- Control identification, risk quantification or qualification has not occurred, nor have recommendations been provided to management regarding additional control measures.
- A small number of senior managers recognize that ISRA is an issue that must be addressed.
- Some information technology groups or operations departments may have identified an employee to deal with an ISRA component or action item.

Key Element	Characteristics
Identify Business Processes	Some departments may have identified key functions and systems as part of DR plan, but is likely incomplete.
Prioritize Business Processes	Prioritized for continuity and recovery purposes.
Identify Assets	Informal list prepared, likely part of DR plan. Narrow focus, perhaps on IT assets only.
Identify Threats	Informal list prepared, likely part of DR plan. Very limited understanding at the management and executive level of the threats to the environment that would most seriously impact the corporate's viability.
Identify Existing Controls	Not documented or incomplete.
Identify Vulnerabilities	Informal list prepared, likely part of DR plan. Very limited understanding at the management and executive level of the threats to the environment that would most seriously impact the corporate's viability.
Risk Determination	Not considered
Develop Security Management Strategy	Not considered
Residual Risk Identification	Not considered
Risk Monitoring and Reporting	Not considered

Level 2 - Repeatable

Characteristics:

- A limited ISRA is performed periodically, but the process is still immature and developing.
- An internal methodology with templates exists, though they may not be complete or consistently utilized/applied.
- Assets, threats and vulnerabilities are documented, but primarily at the information technology level. Some identification of existing controls and risk qualification is evident.
- Recommendations for additional controls or risk mitigation actions may be provided to a responsible manager or group of managers, but this does not have the full attention of executive management.
- The process to manage findings and update the ISRA may be poor or nonexistent. There is no centralized approach or commitment.
- There is an emerging and sustained understanding among management that information security risks are important and need to be considered.
- There is an individual responsible for the ISRA, but this may not be consistent with his/her primary position responsibilities.
- There is no formal training for those involved, so significant variations in quality result as skill development is left to individuals.

Key Element	Characteristics
Identify Business Processes	A corporate-wide business continuity BIA has been completed, identifying all business processes.
Prioritize Business Processes	Some attempt has been made to prioritize for GLBA data, but the prioritization is primarily for continuity and recovery purposes.
Identify Assets	Identified and documented, but limited to IT. Does not represent all corporate assets.
Identify Threats	Identified and documented, but limited. Emerging and sustained understanding among management that information security threats are important and need to be considered.
Identify Existing Controls	Identified and documented, but limited to IT.
Identify Vulnerabilities	Identified and documented, but limited. Emerging and sustained understanding among management that information security vulnerabilities are important and need to be considered.
Risk Determination	Some risk qualification is evident, but may be part of a project or done by a few departments. Not on an organizational level.
Develop Security Management Strategy	Some management action plans are drafted to address the risk issue, but may not be consistent with an overall information system strategy and may not have included the involvement of appropriate management.
Residual Risk Identification	Some residual risk qualification is evident.

Risk Monitoring and Reporting	Some ongoing monitoring of management action plans is performed, but primarily on an ad hoc level.
--------------------------------------	--

Level 3 - Defined

Characteristics:

- An organization-wide information security risk assessment is performed annually, utilizing a written and repeatable methodology, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and published regulatory guidance.
- Business processes/assets are prioritized based upon the existence of GLBA data as well as the criticality to the corporate.
- A central list of assets, threats and vulnerabilities has been documented.
- Existing controls have been formally identified, and a qualitative assessment of identified risks has occurred.
- Detailed risk assessments of business processes, systems and/or applications have been scheduled and assessments of critical assets are in process.
- There is an individual responsible for the ISRA, with responsibility for information security.
- This individual has received ISRA training, relative to the standard methodology adopted by the corporate. Variations in quality may still result as skill development is left to individuals, but is improving.
- A formal organization oversees the risk management process and findings and recommendations for additional controls or risk mitigation actions are reported to executive management and the Board consistent with existing corporate reporting structures.
- The risk assessment supports information security programs and testing plans and is a primary input into the information security strategic planning.
- Risk assessments are regularly utilized to support implementation of cost-effective controls.
- Processes have been defined to pro-actively update risk assessments based upon identified triggers and emerging risks.

Key Element	Characteristics
Identify Business Processes	A corporate-wide business continuity BIA has been completed, identifying all business processes.
Prioritize Business Processes	Prioritized based upon the confidentiality (GLBA), integrity and availability requirements of the information.
Identify Assets	A defined process for identifying assets across the corporate, not just in IT, is utilized.
Identify Threats	A defined process to identify information security threats across the corporate is utilized. Changes in threat environment trigger updates to the threat list.
Identify Existing Controls	Existing controls have been formally identified and documented.
Identify Vulnerabilities	A defined process to identify both organizational and technical information security vulnerabilities corporate-wide is utilized. This process includes pro-actively monitoring new vulnerabilities.
Risk Determination	A qualitative assessment of identified risks is completed, which includes the impact to GLBA data and critical corporate processes.

Develop Security Management Strategy	Management action plans are drafted to address additional controls for risk mitigation and are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structure.
Residual Risk Identification	Residual risk has been qualified and communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structure.
Risk Monitoring and Reporting	A monitoring and reporting structure has been developed and implemented. Progress reports are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.

Level 4 - Managed

Characteristics:

- An organization-wide information security risk assessment is performed annually consistent with an industry standard methodology (OCTAVE, NIST, etc.) and published regulatory guidance.
- The corporate has completed detailed risk assessments of critical business processes, systems and/or applications and has established processes for updating the same on a scheduled basis or when any significant changes are made.
- Changes in threat environment triggers update to threat list.
- A central list of assets, threats and vulnerabilities exists, and a process has been implemented to update these lists for changes in the risk environment,
- Existing controls have been formally documented.
- A formal qualitative assessment of identified risks has occurred, which is consistent with industry standards and published regulatory guidance.
- Lead responsibility for performing the ISRA is assigned to a trained internal information security analyst, or is contracted out to an experienced third-party/vendor.
- A formal process exists for managing and reporting findings.
- Executive sponsorship exists for the information security risk management process, and findings and recommendations for additional controls or risk mitigation actions are reported to management, executive management and the Board, consistent with existing corporate reporting structures.

Key Element	Characteristics
Identify Business Processes	All business processes have been identified and documented, consistent with an industry standard methodology (OCTAVE, NIST, etc), and in consideration of published regulatory guidance.
Prioritize Business Processes	Prioritized based upon the confidentiality (GLBA), integrity and availability requirements of the information.
Identify Assets	A central list of assets has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and in consideration of published regulatory guidance.
Identify Threats	A central list of threats has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and in consideration of regulatory guidance. Changes in threat environment triggers update to threat list.
Identify Existing Controls	A central list of identified controls is documented, consistent with an industry standard methodology (OCTAVE NIST, etc.) and in consideration of regulatory guidance.
Identify Vulnerabilities	A central list of vulnerabilities has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and in consideration of regulatory guidance. Includes technical scans and code reviews.

	Procedures have been established to update the vulnerability list as new vulnerabilities are discovered.
Risk Determination	A formal qualitative or quantitative assessment of identified risks has occurred, consistent with industry standard methodology and published regulatory guidance.
Develop Security Management Strategy	A formal qualitative or quantitative assessment of identified risks has occurred, consistent with industry standard methodology and published regulatory guidance.
Residual Risk Identification	Formal management action plans are drafted to address additional controls for risk mitigation and these plans are congruent with an overall information system strategy. Action plans are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structure.
Risk Monitoring and Reporting	A formal process has been defined for monitoring and reporting on risk mitigation strategies and is communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.

Level 5- Optimized

Characteristics:

- An organization-wide information security risk assessment is performed at least annually or as changes in the corporate's technology/business process environments occur.
- The corporate has completed detailed risk assessments of all business processes, systems and/or applications and updates the same on a scheduled basis or when any significant changes are made.
- The ISRA adheres to an industry standard methodology (OCTAVE, NIST, etc.) and meets all regulatory guidance.
- A formal qualitative or quantitative assessment of identified risks has occurred, which is consistent with industry standards and published regulatory guidance.
- ISRA is reflective of a mature and proactive information security program, and part of an organizational culture with a risk management focus.
- Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented.
- Senior executives can articulate the ISRA strategy and they see ISRA as a value-added contribution to the enterprise.
- Transfer of knowledge regarding information security risk management practices has occurred throughout the organization; thus, management is not reliant on a select group of individuals.

Key Element	Characteristics
Identify Business Processes	All business processes have been identified and documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and meeting all published regulatory guidance.
Prioritize Business Processes	Prioritized based upon the confidentiality (GLBA), integrity and availability requirements of the information.
Identify Assets	A central list of assets has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and meets all published regulatory guidance.
Identify Threats	A central list of threats has been documented, consistent with an industry standard methodology (OCTAVE NIST, etc.) and in consideration of regulatory guidance. Threat list is updated as changes in the organizations technology/business process environments occur. Information on new threats are systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented.
Identify Existing Controls	A central list of identified controls is documented, consistent with an industry standard methodology (OCTAVE NIST, etc.) and in consideration of regulatory guidance. System controls are specifically designed to ensure a minimized level of risk exposure is present, and is

	part of an organizational risk management focus.
Identify Vulnerabilities	A central list of vulnerabilities has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and meets all regulatory guidance. Information on new vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented
Risk Determination	A formal qualitative or quantitative assessment of identified risks has occurred, consistent with industry standards and regulatory guidance. Risk calculations include input from business units. This risk information is considered as part of an organizational risk management focus.
Develop Security Management Strategy	Formal management action plans are drafted to address additional controls for risk mitigation and these plans are congruent with an overall information system strategy. Action plans are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structure.
Residual Risk Identification	A formal qualitative or quantitative residual risk assessment has occurred, consistent with industry standards and regulatory guidance. Risk calculations include input from business units. This risk information is considered as part of an organizational risk management focus.
Risk Monitoring and Reporting	A formal process has been defined for monitoring and reporting on risk mitigation strategies which are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.

CMM Matrix

Level	Identify Business Processes	Prioritize Business Processes	Identify Assets	Identify Threats	Identify Existing Controls	Identify Vulnerabilities	Risk Determination	Develop Security Management Strategy	Residual Risk Identification	Risk Monitoring and Reporting
0	No	No	No	No	No	No	No	No	No	No
1	Some departments may have identified key functions and systems as part of DR plan, but is likely incomplete.	Prioritized for continuity and recovery purposes.	Informal list prepared, likely part of DR plan. Narrow focus, perhaps on IT assets only.	Informal list prepared, likely part of DR plan. Very limited understanding at the management and executive level of the threats to the environment that would most seriously impact the corporate's viability.	Not documented or incomplete.	Informal list prepared, likely part of DR plan. Very limited understanding at the management and executive level of the threats to the environment that would most seriously impact the corporate's viability.	Not considered.	Not considered.	Not considered.	Not considered.
2	A corporate-wide business continuity BIA has been completed, identifying all business processes.	Some attempt has been made to prioritize for GLBA data, but the prioritization is primarily for continuity and recovery purposes.	Identified and documented, but limited to IT. Does not represent all corporate assets.	Identified and documented, but limited. Emerging and sustained understanding among management that information security threats are important and need to be considered.	Identified and documented, but limited to IT.	Identified and documented, but limited. Emerging and sustained understanding among management that information security vulnerabilities are important and need to be considered.	Some risk qualification is evident, but may be part of a project or done by a few departments. Not on an organizational level.	Some management action plans are drafted to address the risk issue, but may not be consistent with an overall information system strategy and may not have included the involvement of appropriate management.	Some residual risk qualification is evident.	Some ongoing monitoring of management action plans is performed, but primarily on an ad hoc level.

CMM Matrix (continued)

Level	Identify Business Processes	Prioritize Business Processes	Identify Assets	Identify Threats	Identify Existing Controls	Identify Vulnerabilities	Risk Determination	Develop Security Management Strategy	Residual Risk Identification	Risk Monitoring and Reporting
3	A corporate-wide business continuity BIA has been completed, identifying all business processes.	Prioritized based upon the confidentiality (GLBA), integrity and availability requirements of the information.	A defined process for identifying assets across the corporate, not just in IT, is utilized.	A defined process to identify information security threats across the corporate is utilized. Changes in threat environment trigger updates to the threat list.	Existing controls have been formally identified and documented.	A defined process to identify both organizational and technical information security vulnerabilities corporate-wide is utilized. This process includes pro-actively monitoring new vulnerabilities.	A qualitative assessment of identified risks is completed, which includes the impact to GLBA data and critical corporate processes.	Management action plans are drafted to address additional controls for risk mitigation and are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structure.	Residual risk has been qualified and communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structure.	A monitoring and reporting structure has been developed and implemented. Progress reports are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.

CMM Matrix (continued)

Level	Identify Business Processes	Prioritize Business Processes	Identify Assets	Identify Threats	Identify Existing Controls	Identify Vulnerabilities	Risk Determination	Develop Security Management Strategy	Residual Risk Identification	Risk Monitoring and Reporting
4	All business processes have been identified and documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) And in consideration of published regulatory guidance.	Prioritized based upon the confidentiality (GLBA), integrity and availability requirements of the information.	A central list of assets has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and in consideration of published regulatory guidance.	A central list of threats has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and in consideration of regulatory guidance. Changes in threat environment triggers update to threat list.	A central list of identified controls is documented, consistent with an industry standard methodology (OCTAVE NIST, etc.) and in consideration of regulatory guidance.	A central list of vulnerabilities has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and in consideration of regulatory guidance. Includes technical scans and code reviews. Procedures have been established to update the vulnerability list as new vulnerabilities are discovered.	A formal qualitative or quantitative assessment of identified risks has occurred, consistent with industry standard methodology and published regulatory guidance.	Formal management action plans are drafted to address additional controls for risk mitigation and these plans are congruent with an overall information system strategy. Action plans are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.	A formal process has been defined for identifying residual risk and communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.	A formal process has been defined for monitoring and reporting on risk mitigation strategies which are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.

CMM Matrix (continued)

Level	Identify Business Processes	Prioritize Business Processes	Identify Assets	Identify Threats	Identify Existing Controls	Identify Vulnerabilities	Risk Determination	Develop Security Management Strategy	Residual Risk Identification	Risk Monitoring and Reporting
5	All business processes have been identified and documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and meeting all published regulatory guidance.	Prioritized based upon the confidentiality (GLBA), integrity and availability requirements of the information.	A central list of assets has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and meets all published regulatory guidance.	A central list of threats has been documented, consistent with an industry standard methodology (OCTAVE NIST, etc.) and in consideration of regulatory guidance. Threat list is updated as changes in the organizations technology/business process environments occur. Information on new threats are systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented.	A central list of identified controls is documented, consistent with an industry standard methodology (OCTAVE NIST, etc.) and in consideration of regulatory guidance. System controls are specifically designed to ensure a minimized level of risk exposure is present, and is part of an organizational risk management focus.	A central list of vulnerabilities has been documented, consistent with an industry standard methodology (OCTAVE, NIST, etc.) and meets all regulatory guidance. Information on new vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented.	A formal qualitative or quantitative assessment of identified risks has occurred, consistent with industry standards and regulatory guidance. Risk calculations include input from business units. This risk information is considered as part of an organizational risk management focus.	Formal management action plans are drafted to address additional controls for risk mitigation and these plans are congruent with an overall information system strategy. Action plans are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structure.	A formal qualitative or quantitative residual risk assessment has occurred, consistent with industry standards and regulatory guidance. Risk calculations include input from business units. This risk information is considered as part of an organizational risk management focus.	A formal process has been defined for monitoring and reporting on risk mitigation strategies which are communicated to the appropriate level of management and/or the board consistent with existing corporate reporting structures.

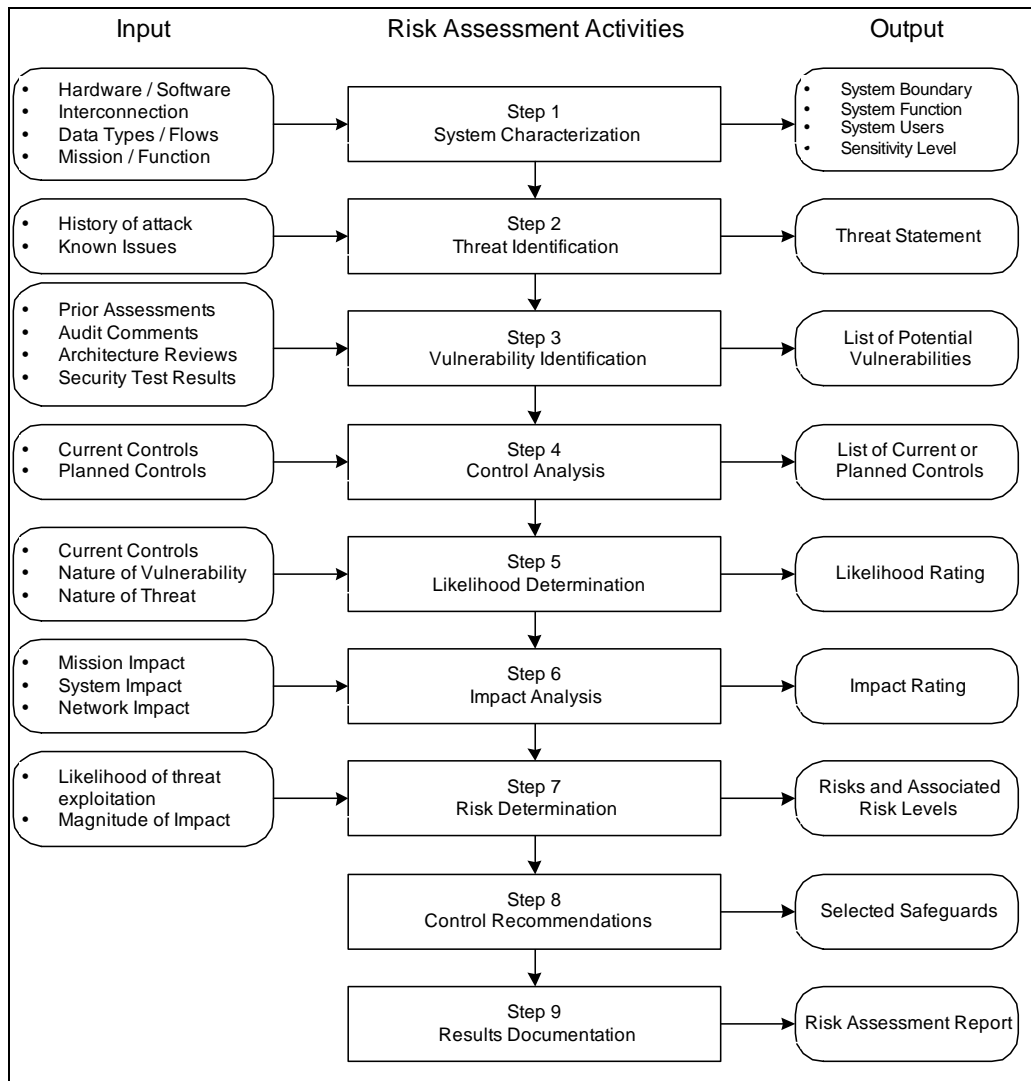
Reference Materials

Terminology

Term	Definition
Application Information Security Risk Assessment	An application information security risk assessment focuses on the discrete systems and/or applications involved in a process with established boundaries. The application information security risk assessment typically involves significantly more detail and analysis than an organizational information systems risk assessment.
Asset	References such tangible items as servers, routers, facilities, people, data and may include such intangible features such as morale, reputation, or intellectual property.
Enterprise Risk Assessment	An enterprise risk assessment generally refers to the overall risk position of the entity and is much broader than an information security risk assessment. In addition to risk to the assets of the entity, it would include such areas as credit risk, operational risk, natural disasters, etc.
Independent	Individuals not involved in the day-to-day development, maintenance and operation of the asset under review (e.g. internal audit, external third-parties, information security staff, etc).
Information Security Risk Assessment	An information security risk assessment is a process of information gathering and analysis aimed at determining the risk levels of information assets. This is done by identifying risks to information system security and determining the probability of occurrence and the resulting impact on the organization, and by recommending additional safeguards to further mitigate the risk.
Organizational Information Security Risk Assessment	An organizational information security risk assessment is a high level assessment of a corporate's information security program. In performing an initial organizational information security risk assessment, the institution would identify and group all information assets for analysis. Logically grouping such assets as a system or business process is recommended. As part of the organizational risk assessment; management should also identify those practices (i.e. physical security; HR practices) that should be consistent across the organization, regardless of business process. These should not need to be reassessed for each application, but instead could be addressed once, for the organization as a whole, although exceptions can exist.
Residual Risk	Measure of actual risk of an information system given the consideration of existing controls.
Risk	Occurs when there is the potential for a threat to exploit vulnerability.
Risk Determination	Assigning a risk level to a threat/vulnerability pair, given the likelihood and impact. The risk level represents the degree of risk to which an information asset might be exposed if a given vulnerability were exploited.

Safeguards	Existing controls or additionally recommended controls that are aimed at either reducing threats or reducing vulnerabilities.
System	A system includes the software (application), hardware, databases, interfaces, etc. required to employ the capabilities of a computer directly to a task that the user wishes to perform. For example, a wire system may be comprised of a number of servers and software applications that accept wire instructions from various sources (i.e. CCUN/ OpenDoor and CNECS/Corporate Explorer), pass the wire to the PAYPlus system which sends it to the Federal Reserve. The PAYPlus system then prepares a posting file to post the wire to CCUN or CNECS as is appropriate. Each of the discrete systems involved in the process allows management to establish system boundaries and review the entire wire processing process.
Threat	Any circumstance or event with the potential to cause harm to an IT system. These can be natural, human, or environmental.
Vulnerability	A flaw or weakness in information system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and results in destruction, disclosure, or modification of information.

NIST Risk Assessment Methodology



OCTAVE Risk Assessment Methodology

Phase 1: Build Asset-Based Threat Profiles

Process S1: Identify Organizational Information

- S1.1: Establish impact evaluation criteria (Step 1)
- S1.2: Identify organizational assets (Step 2)
- S1.3: Evaluate organizational security practices (Steps 3 – 4)

Process S2: Create Threat Profiles

- S2.1: Select Critical Assets (Steps 5 – 9)
- S2.2: Identify security requirements for critical assets (Steps 10 – 11)
- S2.3: Identify threats to critical assets (Steps 12 – 16)

Phase 2: Identify Infrastructure Vulnerabilities

Process S3: Examine the Computing Infrastructure in Relation to Critical Assets

- S3.1: Examine access paths (Steps 17 – 18)
- S3.2: Analyze technology-related processes (Steps 19 – 21)

Phase 3: Develop Security Strategy and Plans

Process S4: Identify and Analyze Risks

- S4.1: Evaluate impact of threats (Step 22)
- S4.2: Establish probability evaluation criteria (Step 23)
- S4.3: Evaluate probabilities of threats (Step 24)

Process S5: Develop Protection Strategy and Mitigation Plans

- S5.1: Describe current protection strategy (Step 25)
- S5.2: Select mitigation approaches (Steps 26 - 27)
- S5.3: Develop risk mitigation plans (Step 28)
- S5.4: Identify changes to protection strategy (Step 29)
- S5.5: Identify next steps (Step 30)

Appendix A (Business Processes)

Sample Listing – Business Processes

This listing was compiled to serve as an example only. This list is representative of Corporate Network business processes, but is not considered to be all inclusive.

Accounts Payable	International Services
Adjustments	Investment Advisory Services
Application Development and Support	Investment Accounting
Asset/Liability Accounting	Item Processing
Asset/Liability Management	Help Desk
Asset Management	Human Resource Administration
ATM Processing	Loan Purchasing
Automated Clearing House (ACH) Processing	Loan Processing
Bill Payment	Marketing
Board Reporting	Member Relations
Brokerage Services	Member Account Maintenance
Cash Management	Member Account Transfers
Certificate Account Processing	Market Risk Analysis
Check Collection	Network Administration
Coin & Currency	Overnight Loans
Computer Applications	Overnight Investments
Corporate Services	Payroll Administration
Credit Card Processing	Public Relations
Credit Review & Monitoring	Regulatory Reporting
Data Entry	Returns Processing
Debit Card Processing	Security Safekeeping
Derivative Accounting	Security Administration
End User Services	Settlement Processing
Facilities Management	Share Account Processing
Fed Account Reconciliation	Share Draft Processing
Foreign Collections and Research	Transfer Processing
General Ledger Account Reconciliation	Western Union Transfers
Incident Management	Wire Processing

Appendix B (Asset Listing)

Sample Asset Listing

This listing was compiled to serve as an example only. This list is representative of Corporate Network assets, but is not considered to be all inclusive.

ACH Files	Fedline Terminal
ADP Software	InTrader
Anti-virus software	Intrusion Detection Software
A/S 400	JHA
APEX-ACH	Microsoft Office Software
Backup Tapes	Modem(s)
Batch Processing Software	Navision Accounting Software
Brocade Fiber Channel Switch	Non-public personal information (NPI) data
Catalyst 4500 L3 Switch	PayPlus Application
CCUN	PGP Software
CCUN 400	OFS
CCUN X Files Trickle	Open Door Application
Checks	Oracle Database
Check Images	SQL 2000 Database
Checkpoint Firewall	Solaris server v9.0
CISCO Pix Firewall	T1 Lines
CISCO 7507 Routers	Vendor Routers
CISCO 6509 Switches	Websense
CNECS	Windows 2000 SQL Server
Corporate Explorer	Windows 2000 Server
Corporate Facility	Windows 2000 App Server
Customer Data (Member)	Windows XP Workstations
EDS	Windows 2000 Web Server
Employees	Windows 2000 Internal Server

Appendix C (Threat Listing)

Sample Threat Listing

This listing was compiled to serve as an example only. This list is representative of Corporate Network threat sources, but is not considered to be all inclusive.

THREAT TYPES	THREAT ACTION
Natural Threats:	
Cold, extreme	Temperature damages infrastructure and impairs equipment, machines, and vehicles. Building damage, environment unsuitable for staff, unable to receive or deliver products and components, staff unable to commute.
Drought	Dry plants and shrubs can be a fire hazard. Normal use of water during a drought can reduce water tables and water pressure than can hamper fire response efforts.
Electrical storm	Lightning strikes can cause direct damage or secondary fire risks. Strikes to the ground, wire cabinets, or overhead wires can damage electrical and communications components.
Epidemic	A pandemic can cause widespread loss of life and invoke quarantine directives. Virus outbreaks can be possibly spread through air, ingestion, and contact.
Extraterrestrial Impact	The collision of earth by a large asteroid or comet could result in a massive and long lasting change to life on earth. The probability is small, the impact beyond comprehension, and the controls are of unknown effectiveness. Such an event would make business continuity a non-issue.
Fire external	An external fire can cause widespread damage if left to continue to burn. Fire can feed and grow on available fuel sources and favorable weather conditions.
Fire internal	An internal fire is one of the most common causes for large-scale damage to the workplace. Equipment and infrastructure failures can cause an internal fire. Mishandling of combustible materials and other elements of combustion can also initiate a fire situation.
Flooding external	External flooding is usually caused by excessive rain and seasonal storms. It can also be caused by failures of water control entities such as dams, locks, river controls, and other infrastructure failures.

Flooding internal	Internal flooding is another common cause of damage to the workplace. Damage can occur from infrastructure failure of water pipes, fire suppression systems, sanitation system failures, kitchen and break area appliance failures, and tenant actions. Roof, ceilings, doors, and walls can also allow external water into the workplace.
Heat, extreme	Extreme heat can lead to drought conditions. It can also overload electrical power grids. Continuous exposure to extreme heat may impact the health of staff.
Hurricane	Hurricanes can cause wide-spread damage from flooding, tornadoes, wind driven debris, and infrastructure failures.
Landslide or subsidence	Shifting of the ground can cause substantial damage to structures and change the surrounding lay of the land. A significant occurrence could result in the structure being destroyed or uninhabitable for a considerable length of time.
Seismic damage	Seismic activity can cause damage to buildings, city infrastructure, and essential services. The nearest large tectonic fault is the New Madrid fault in the six-state area that includes southern Illinois.
Snow or ice storm	Snow and ice accumulation can damage infrastructure due to weight loads and complicate logistics in keeping transportation routes open. Building damage, external conditions unsuitable for staff, inability to receive or deliver products and components, staff unable to commute.
Tidal wave	A dramatic increase in water level could cause damage from flooding, erosion, water weight and pressure.
Tornado	Tornadoes cause localized to wide-spread devastation from spiraling winds well over 100 miles per hours containing debris that add to its destructive forces.
Typhoon	Typhoons in the Pacific and cyclones in the Indian Oceans have the same threat characteristics as a hurricane in the Atlantic Ocean.
Volcano	Volcanoes can cause significant seismic and damage, generate rivers and flows of molten rock and lave, and spew vast amounts of ash, dust, and other debris into the upper air layers.
Wind damage	Sustained winds and gusts can cause wide-spread damage.
Human Threats:	
Arson	The intentional burning of a building or its contents.
Blackmail/extortion	Use of criminal means to obtain property by consent.
Bomb	The detonation of an explosive devise to cause physical damage to a structure, its contents, and/or its staff.
Burglary	The breaking in and committing of a felony.

CBR release	The release of chemical, biological, radiological agents are associated with terrorist activities. This action can also occur as the result of an accident during manufacture, use in commercial processes, or transportation.
Civil disorder	Civil disorder is the unlawful assemblage and violence of a number of persons, which are attended with injury to the persons or property, or terror and alarm to the neighborhood in which it takes place.
Error, unintentional	Errors as a result of operational, procedural, instructional, and/or other processes.
Embezzlement	The wrongful or willful taking of money or property belonging to someone else after the money or property has lawfully come into the possession or control of the person taking it.
Explosion	The detonation of any chemical compound mixture, or device, the primary or common purpose of which is to function by explosion; the term includes, but is not limited to, dynamite and other high explosives, black powder, pellet powder, initiating explosives, detonators, safety fuses, squibs, detonating cord, igniter cord, and igniters.
Fraud	An intentional misrepresentation of material existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage. Fraud may also include an omission or intentional failure to state material facts, knowledge of which would be necessary to make other statements not misleading.
Hazardous material	The release of hazard material can occur as the result of an accident during manufacture, use in commercial processes, or transportation.
Health hazard	A health hazard can result in the illness of staff from workplace or environmental situations.
Hostage	The forcible and unlawful abduction and conveying away of a man, woman or child, from his or her home, without his or her will or consent and sending such person away with an intent to deprive him or her of some right. This
Improper handling of sensitive data	Confidentiality of sensitive information has grown in importance as larger quantities of this information exist in electronic format and at more businesses. It is also processed and transported in greater frequency. Laws and regulations have intensified the need for proof of protection of customer data and disclosure if confidentiality is compromised.
Kidnapping	The forcible and unlawful abduction and conveying away of a man, woman or child, from his or her home, without his or her will or consent and sending such person away with an intent to deprive him or her of some right.

Litigation	The process of bringing and pursuing a lawsuit.
Malicious damage or destruction of physical assets	See arson, bomb, explosion, sabotage, and vandalism.
Malicious damage or destruction of software or data	The altering, replacing, or deleting of software code and/or information can result in loss of integrity, inaccurate results, and unavailability of intellectual resources.
Negative publicity	Negative publicity is delivered to huge numbers is a near instantaneous fashion.
Robbery or theft	The felonious and forcible taking from the person of another, goods or money to any value, by violence or putting him in fear.
Sabotage	The destruction of an employer's property (as tools or materials) or the hindering of manufacturing by discontented workers
Safety hazard	A safety hazard can result in the injury or death of staff from workplace or environmental situations.
Terrorism	An activity directed against persons involving violent acts or acts dangerous to human life which would be a criminal violation if committed within the jurisdiction of the U.S.; and is intended to intimidate or coerce a civilian population.
Unauthorized access to data or theft of data	The copying, viewing, or theft of software code and/or information can result in loss of confidentiality; identify protection, and the competitive edge of intellectual resources.
Unauthorized modification of software or hardware	The copying, viewing, or theft of software code and/or information can result in loss of confidentiality, identify protection, and the competitive edge of intellectual resources.
Unauthorized physical access	Physical access to corporate offices can exploit vulnerabilities that are normally protected by security controls. Damage, theft, physical harm, and surveillance are all possible threat actions.
Vandalism	The willful or malicious destruction or defacement of public or private property.
Work stoppage	The halting of normal business activities to draw attention to workplace situations such as contract negotiations, employer-employee relations, and worker representation.
Workplace violence	An offense in the workplace that is a felony and has as one of its essential elements the use, attempted use, or threatened use of physical force against the person or property of another, or an offense that by its very nature involves a substantial risk that such physical force may be used in the course of committing the offense.

Technical Threats:	
Aircraft incident	Impact to physical property resulting in severe damage.
Application software malfunction or failure	Application software failure can cause stoppage of our critical business processes. Normal day-to-day operations revolve around application software. The majority of member interaction occurs through application software. Even phone transactions are completed by corporate staff using application software.
Electromagnetic interference	The occurrence of electromagnetic interference can come from accidental or deliberate actions. Minor incidents can occur from the mishandling of magnetic media near unsafe objects and areas. A deliberate action has been publicized as a terrorist or malicious act to destroy electronic components and data.
Equipment Failure - Non-IS hardware	The corporate critical business processes are dependent upon equipment that resides outside of the management of Information Systems. Failure of this equipment can threaten these business processes.
Fuel shortage	Recent international competition for fuel has impacted the cost and supply of fossil fuels. A short interruption in the supply chain, or continued sharp rises in cost will impact business operations.
Hardware malfunction or failure	Failures of IS hardware can impact the availability of data and operation of key business operations. In order to meet business availability performance commitments, restarting of computers and other hardware can clear-up problems sooner by incurring a shorter interruption to restart instead of longer diagnostic time to find the real problem.
Heating, ventilating or air conditioning failure	HVAC failure may force the relocation of staff and business operations.
Natural gas malfunction or failure	Recent international competition for fuel has impacted the cost and supply of fossil fuels. A short interruption in the supply chain, or continued sharp rises in cost will impact business operations. This threat-risk is becoming a more important factor to business and the public. Loss of natural gas will halt the operation of heating systems at any corporate office. It can also impact facilities of members, vendors, and partners.
Telephone malfunction or failure	Telephone failure can halt severely impact the ability to communicate with members, partners, vendors, and staff. Like the Internet, telephones are the front line image of many business processes.
Power failure/ fluctuations	Sudden loss of power can halt equipment operation. Power loss or fluctuation can damage electrical components and/or affect the performance.

Sanitation system malfunction or failure	A failure of the water and/or sanitation system can halt staff operations. Such failures can threaten the health of staff, damage office infrastructure, and force the shutdown of the physical facility. .
Security system malfunction or failure	The failure of the information security can compromise business assets. Controls to prevent, detect, and respond to security threats could be impaired or cease to function.
System software malfunction or failure	Failures of IS systems software can impact the availability of data and operation of key business operations. In order to meet business availability performance commitments, restarting of systems software can clear-up problems sooner by incurring a shorter interruption to restart instead of longer diagnostic time to find the real problem.
Telecommunications malfunction or failure	Telecommunications failure can halt communications to Internet connections and direct links between corporate and vendor sites.
Transportation malfunction or failure	Transportation failure can halt the transportation of business components and staff.
Backup power malfunction or failure	Sudden loss of power can halt equipment operation. Power loss or fluctuation can damage electrical components and/or affect the performance.
Vehicle incident	See hazardous material and transportation failure.
Water supply malfunction or failure	A failure of the water and/or sanitation system can halt staff operations. Such failures can threaten the health of staff, damage office infrastructure, and force the shutdown of the physical facility.

Appendix D (Vendor Listing)

Risk Assessment Vendors

The vendors noted below provide assistance in performing information security risk assessments. Their inclusion in this document does not constitute a corporate network endorsement or recommendation, but are provided for information only.

Foundstone, a Division of McAfee

Foundstone Corporate Headquarters
27201 Puerta Real, #400
Mission Viejo, CA 92691
877.91.FOUND (877.913.6863)
949.297.5600
949.297.5575 | fax
www.foundstone.com

Visconti Consulting, LLC

5422 Shoalwood Avenue
Austin, Texas 78756
(512) 413-1216

Lambert and Associates

Sandy Lambert, Managing Partner
(323) 469-6978 office
sandra.lambert@lambert-associates.com
www.lambert-associates.com

MicroSolved, Inc.

Attn: John Davis
630 North Hague Avenue, Suite B
Columbus, OH 43204
(614) 351-1237 ext. 205

PricewaterhouseCoopers (security consulting)

Thomas Phelps IV, Director
350 S. Grand Ave.
Los Angeles, CA 90071(213) 217-3577 office
(626) 590-9995 mobile
thomas.phelps@us.pwc.com
www.pwc.com/security

SecureWorks

Attn: Jeff Guggenheim
11 Executive Park Drive, NE
Atlanta, GA 30329
(877)905-6661