# LETTER TO CREDIT UNIONS

## NATIONAL CREDIT UNION ADMINISTRATION
## 1775 Duke Street, Alexandria, VA

**DATE: December 2002**

**LETTER NO.: 02-CU-17**

**TO: All Federally-Insured Credit Unions**

**SUBJ: e-Commerce Guide for Credit Unions**

**ENCL: e-Commerce Guide for Credit Unions (in PDF Format)**

The purpose of this letter is to provide NCUA's e-Commerce Guide for Credit Unions.

The guide offers information to assist credit unions engaging in, or considering, e-Commerce activities (electronic delivery of financial services via the Internet). Credit unions can use this information as a guide to aid in the planning, contracting, delivery, and support of e-Commerce activities.

Offering e-Commerce services may provide benefits to credit unions and their members. However, the use of the Internet can also increase the amount of risk to the credit union. The enclosed guide focuses on processes to assist credit unions in managing the risks related to e-Commerce.

If you have any questions, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/S/

Dennis Dollar
Chairman


# e-Commerce Guide For Credit Unions

NCUA 8072 November 2002

# Table of Contents

# 1. INTRODUCTION

The National Credit Union Administration (NCUA) has developed this guide to assist credit unions engaging in, or considering, e-Commerce activities. For the purposes of this guide, e-Commerce is defined as the electronic delivery of financial services via the Internet. NCUA does not expect all credit unions to offer e-Commerce. However, NCUA expects credit unions offering e-Commerce to do so in a safe and sound manner.

This guide focuses on **processes** to assist credit unions in managing the risks related to e-Commerce in an environment of rapidly changing technology. Credit union management should use the information in this guide to assist with technology planning, contracting, delivery, and support of e-Commerce activities. This should be done within a framework designed to identify, quantify and, to the extent possible, reduce related technology risks.

Much of the information in this guide is derived from NCUA issuances such as Rules & Regulations and Letters to Credit Unions. Although this information is provided in summary format in the guide, the related issuances typically contain more detail on a particular subject and may contain additional checklists that can assist in evaluating performance in a given area. Please refer to Appendix A for a listing of NCUA reference information. These issuances, as well as additional guidance, can be found via the Information Systems and Technology link under the reference section of the NCUA website (http://www.ncua.gov)*. This site is updated frequently and can serve as a valuable resource.

One of management's fundamental responsibilities in the Information Systems and Technology (IS&T) area is to ensure adequate internal controls over information (data) and the systems (hardware & software) that store, process, and transport it. While all credit union officials and staff will not become experts in information systems, the board of directors, supervisory or audit committee, and operating management should understand the risks and controls associated with the information systems used by the credit union.

This guide is designed to assist credit union officials, management, and staff responsible for aspects of information technology. However, it may also prove useful for others (e.g., auditors, service providers, affiliates, business partners, etc.) when completing evaluations of information technology security and controls related to credit union electronic financial services.

** Some credit unions utilize NCUA's IS&T exam program (located on the website) to assist with a self-review. Be aware that the electronic version of the questionnaires has a help textbox feature. Moving a cursor over the red triangle in the corner of the cells for many of the exam steps will reveal text boxes that further explain the review step.*

## 2. THE CONVERGENCE OF CREDIT UNIONS AND THE INTERNET

Rapid developments in technology are causing credit unions to reevaluate traditional delivery channels and products in order to better serve their members. In fact, the majority of federally insured credit unions now have a presence on the Internet. Many credit unions offer members the ability to initiate transactions on their website and some even offer wireless account access.

Websites are frequently categorized as follows:

- **Informational** – Members can view general information such as loan and share rates, credit union contact information, hours of operation, current promotions, etc.
- **Interactive** – Builds on the capabilities of the informational website by enabling members to also interact with the site to request data (e.g., share and loan balances, account histories) or submit data (e.g., new account or loan application).
- **Transactional** – Builds on the capabilities of the Interactive site by also enabling members to conduct financial transactions (e.g., withdrawal via check issuance, pay bills, make loan payments, transfer funds, etc.).

Some additional Internet-based services credit unions currently offer include:

- **bill payment and presentment** –the ability to receive and schedule payment of bills;
- **account aggregation** – the ability to view all on-line relationships in one consolidated format;
- **statement delivery** – the ability to receive statements on-line;
- **share draft imaging** – the ability to view images of cancelled checks on-line;
- **personal financial management (PFM) files** – the ability to download account histories to software programs (e.g., Quicken, Microsoft Money, etc.) on the user's personal computer (PC);
- **investment services** – the ability to make investments on-line; and
- **purchase services** – the ability to purchase merchandise on-line.

The Internet, as with most services and delivery channels, has inherent risks and potential rewards. On one hand, the Internet can provide the basis for worldwide communication with members and the ability for members to remotely conduct transactions. On the other hand, the Internet provides the potential for anonymous access to credit union member information systems from anywhere in the world resulting in numerous threats, including:

- observation, theft, or destruction of sensitive data;
- insertion of false data or malicious code (e.g. virus, worm, Trojan Horse);
- fraudulent financial transactions;
- performance degradation, disruption of operations (e.g., denial of service attacks); and
- purposeful or inadvertent damaging of systems.

If these threats are not adequately understood and addressed, the credit union (via losses due to fraud, ransom demands, bad press, etc.) and members (via fraud, identity theft, etc.) may incur harm. If the risks are understood and properly mitigated, the credit union and members can realize the rewards (e.g., member retention, wealth of competitive on-line services, etc.).

# 3. SMALL CREDIT UNIONS

Small credit unions report offering informational, transactional, and interactive sites to their memberships. Compared to their larger counterparts, small credit unions may face additional challenges when offering new products or services due to their lower resource levels (e.g., financial capacity, staff levels, technical expertise, etc.). This means that small credit unions will need to do what they already do well – be resourceful.

Fortunately, small credit unions have a long history of effectively using limited resources to serve their members in a safe and sound manner. This resourcefulness is important, because the risks posed by e-Commerce are not solely dependent on the credit union's asset size but rather on its unique environment (i.e., services offered, outside connectivity, use of outsourcing, type of system used, credit union's network architecture, service provider's network architecture, staff technical expertise, financial resources, physical facilities, existing controls, etc.).

**Resources**

As with many initiatives, small credit unions will likely need to rely more heavily (than larger credit unions) on certain resources including:

- **volunteers** (research and service provider evaluation);
- **peer credit unions** (lessons learned and service provider recommendations);
- **mentor credit unions** (technical advice);
- **user groups** (education forums, for leverage in dealing with service providers);
- **sponsor organizations** (technical advice and support);
- **industry organizations, research organizations, and periodicals** (advice via websites, magazines, conferences, research papers, specialty resources for small credit unions);
- **credit union audit organizations** (advice via websites, magazines, conferences, audit programs);
- **service providers** (education as to risks and appropriate control measures necessary at the credit union);
- **bonding companies** (self-assessment checklists, control recommendations based on knowledge of e-Commerce risks from research and bond claims); and
- **regulators** (requirements per regulations, guidance from issuances).

**Resourcefulness**

A small credit union may not have the resources to afford:

- a self-developed Internet banking package, but a service provider may offer one at a reasonable price;

- an in-house e-Commerce solution, but an outsourced solution may be affordable;

- a fully transactional website, but an interactive site may be sufficient;

- an independent assessment of a service provider, but the service provider may obtain one or the combined resources of a user group may be able to pay for one (assuming the service provider authorizes it);

- an independent assessment of its internal e-Commerce environment, but its bonding company may provide a limited review at no cost;

- a paid consultant to perform a compliance review of its website, but may be able to have its mentor credit union's compliance officer make a review and offer recommendations;

- an attack and penetration test, but may be able to afford a limited scope review including basic network scanning and a high-level network vulnerability assessment;

- a paid consultant to develop policies and procedures, but could seek free sample policies from other credit unions or even from reputable security websites, and tailor them for applicability at the credit union;

- a dedicated firewall appliance costing thousands of dollars, but may find an inexpensive, yet appropriate, one that fits its needs; or

- a new high-end PC to use as a stand-alone unit (not networked to any other credit union computers) for web browsing and e-mail, but its sponsor may have an older PC, that would work fine for this purpose, that it may be willing to donate to the credit union.

These are just some examples of lower-cost control measures that might be appropriate given specific threat exposure facing a particular small credit union. Not all controls are necessarily expensive. In fact, some have no cost (i.e., password-protected screensavers that activate after a period of inactivity). It is up to each credit union to go through a process to determine the specific control measures that are appropriate given its unique situation.

There may be cases where a small credit union may go through a feasibility analysis and determine that it does not currently have the resources (human or financial) to safely offer the level of e-Commerce services it would like, or its members may not want or need such services. Additionally, in some cases, there will be competing projects for limited funds and other services may currently be considered a higher priority.

This guide focuses on processes (e.g., oversight, risk assessment, security program development, service provider oversight, etc.) that are equally applicable to credit unions of any size.

# 4. OVERSIGHT

The success of the credit union's e-Commerce initiatives will significantly depend on the adequacy of the oversight provided by the board of directors and senior management.

**Strategic Direction**

The board of directors determines the strategic direction of the credit union. To ensure e-Commerce strategies and goals align with the overall strategies and goals of the credit union, the board of directors should consider creation of an e-Commerce oversight committee. This committee should be comprised of representatives of the various operational areas of the credit union (and thus the committee's size will vary greatly depending on the staffing pattern of the credit union).

The committee should oversee all e-Commerce initiatives (planning, deployment, and monitoring) and periodically provide updates to the board of directors. The committee's responsibilities should include:

- reviewing the implications of e-Commerce on the credit union's strategic plan;
- evaluating member expectations and demands;
- determining resource requirements;
- assessing the risks and required controls, particularly related to information security;
- evaluating internal and/or external expertise needed to support e-Commerce; and
- developing effective policies and procedures covering e-Commerce.

It is important that the audit function be represented on the committee to ensure its awareness of e-Commerce activities and to proactively make control recommendations for consideration by the committee. It is more efficient (and less costly) to address system features and controls in the design phase, then to attempt to retrofit them after implementation.

**Technology Planning**

Credit unions are encouraged to develop a formal planning document (i.e. technology plan, IT strategic plan, etc.) outlining their use of technology. This plan will facilitate alignment between the credit union's overall strategic plan and the technology resources and initiatives used to support it. It provides both an assessment of current credit union technology resources as well as identifies those resources that will be necessary to achieve the goals outlined in the overall strategic plan. The resource assessment should include hard and soft resources (i.e., staffing levels, staff expertise, infrastructure, technology service providers, adequacy of related budgeted amounts, etc.). The plan will provide for prioritization of initiatives and support related expenditures. Documentation for individual initiatives (i.e. supporting strategies, analyses, project plans, etc.) can be referenced to make the document more complete.

The plan should address both short-term and longer-term plans, as well as be updated on periodic basis to remain relevant. Board (or committee) review and approval of the plan will help ensure the plan's direction is accurate and serve to document board-level awareness and support of the plan.

## Policies and Procedures

The board of directors is ultimately responsible for approving the policies of the credit union. It is through policies and the resulting procedures that the board of directors and management control the operations of the credit union. Policies and procedures should be developed or updated to specifically address the impact of e-Commerce on credit union operations and should be reviewed and adjusted as necessary (at least annually). The specific policies and procedures needed for a particular credit union will depend on its particular offerings and environment. See Appendix B for a sample listing of some areas that may need to be addressed in policy.

## Security Program

The board of directors is also responsible for ensuring a written security program is in place that is designed to:

- ensure the security and confidentiality of member records;
- protect against anticipated threats or hazards to the security or integrity of such records;
- protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to members; and
- assist in the identification of persons who commit or attempt such actions and crimes.

Chapter 6 details the development of a credit union security program.

# 5. RISK ASSESSMENT & MITIGATION PROCESS

Credit unions planning to engage in e-Commerce must be prepared to safely integrate financial services and emerging technology. Thus, officials need to review the impact e-Commerce may have on a credit union's overall risk exposure.

**Types of Risk**

Risk is the potential for events, expected or unanticipated, to have an adverse effect on the credit union's earnings or capital. A product or service may expose the credit union to multiple risks. Risks can be categorized in many different ways. Common risk categories related to e-Commerce include:

- **Strategic Risk: Is e-Commerce doing what the credit union intended?**

  This is the risk associated with failure to meet strategic goals due to adverse business decisions, poor implementation, or lack of responsiveness to changes in the environment (credit union, industry, technology, threat, etc.). Without strong managerial capacities and capabilities coupled with adequate monitoring and reporting systems, e-Commerce initiatives may not provide the intended results.

- **Transactional Risk: Is e-Commerce reliable, secure, and transactions valid?**

  This is the risk associated with reliability, fraud or error that results in an inability to deliver products or services, maintain a competitive position, and manage information. This risk, sometimes referred to as operational risk, is largely a function of employee integrity and the internal controls over information systems and operating processes. Without strong controls, the safety and integrity of credit union and member assets may be compromised.

- **Compliance Risk: Is e-Commerce adhering to regulatory, legal, contractual, and other related requirements?**

  This is the risk associated with violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. This risk may also arise in situations where ambiguous or untested laws or rules govern products or services. Without a compliance oversight process, the credit union can face increased exposure to fines, civil money penalties, payment of damages, the voiding of contracts, and diminished reputation.

- **Reputation Risk: Is e-Commerce a public relations liability?**

  This is the risk associated with negative public opinion or perception. Reputation risk affects the credit union's ability to establish new relationships or services, or to continue servicing existing relationships. Failure to adequately manage strategic, operational, or compliance risk, may increase reputation risk and result in litigation, financial loss, or a decline in membership base.

## Risk Assessment & Mitigation Process

One of the primary ways for credit unions to understand and mitigate risks associated with e-Commerce risks is by implementing a thorough risk assessment process. The risk assessment process should be a collaborative effort involving representatives from all areas of the credit union. Although the methodology and format may vary, the process should include the following five critical steps:

1. **Identify internal and external threats which may include employees, hackers, failure of critical service providers, physical disasters, and others that are associated with the type of services provided and the systems used to provide those services.**

   These are the threats that could result in unauthorized disclosure, misuse, alteration, or destruction of credit union or member information or the inoperability of related information processing and delivery systems.

2. **Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity and criticality of credit union and member information.**

   Although some threats may have a low likelihood of occurrence they can have a very significant impact or consequences.

3. **Determine the adequacy of existing controls.**

   Controls include policies, procedures, systems, and other arrangements (e.g., insurance coverage) in place at the credit union. e-Commerce insurance may play an important role in mitigating certain risks within policy limits. However, insurance is not a substitute for strong controls and is unlikely to adequately mitigate reputation risk in the face of a security or privacy breach that becomes publicly known.

4. **Implement enhanced or additional controls as necessary to reduce the e-Commerce related risk to an acceptable level.**

   The board of directors must understand the level of risk exposure associated with e-Commerce in order to effectively control the affairs of the credit union.

5. **Monitor, evaluate (test), adjust, and report on the system of controls to ensure it is operating as intended.**

   The board of directors should be kept apprised of the results of the on-going risk management process.

## Criticality of Data & Systems

Performing an effective risk assessment requires a comprehensive understanding of the value (e.g., degree of sensitivity or criticality) of the systems and information being assessed. This value can be expressed in many different ways; one possible example follows:

- **High** - Extreme liabilities result if the information is compromised (e.g., damaged, destroyed, made public); could cause major financial loss; result in legal action against the credit union; or severely damage the credit union's reputation.

- **Moderate** - Serious liabilities result if the information is compromised; could cause moderate financial loss; legal action against the credit union would be likely; or damage to the credit union's reputation would be moderate.

- **Low** - Liabilities could possibly result if the information is compromised; would likely cause only minor financial loss; litigation unlikely; or damage to the credit union's reputation would be minimal.

That value should be determined for each of the following three protection categories for information and systems:

1. **Integrity** - The information requires protection from unauthorized, unanticipated, or unintentional modification.

2. **Confidentiality** - The information requires protection from unauthorized disclosure.

3. **Availability** - The information or system must be available on a timely basis.

The results of this analysis will assist in determining the necessary protection requirements for the information or system.

## On-going Process

As risk exposure is not static, it is prudent to perform risk assessments on a periodic basis. For example, risk exposure can change quickly with:

- changes in infrastructure (software and hardware);
- advances in technology used by hackers;
- changes to the organizational structure within the credit union;
- discovery of new security vulnerabilities impacting computer systems;
- implementation of new business processes;
- establishment of new service provider relationships (and connectivity); and
- implementation of new products, services, and delivery methods.

Credit unions must monitor industry standards and effective practices in order to ensure their risk mitigation measures continue to be sufficient. Otherwise, the credit union and its members may be subject to excessive risk exposure.

**No One-Size-Fits-All Solution**

Even credit unions of similar asset size and same type of website may have very different environments. The table below shows a very simplified example of just some of the many possible environmental variations for credit unions offering transactional websites to their members.

| | Credit Union A | Credit Union B | Credit Union C |
|---|---|---|---|
| **Type of Website** | **Transactional** | **Transactional** | **Transactional** |
| **Type of Core Share & Loan Processing System** | In-House | Service Bureau On-Line (real-time) | Service Bureau On-Line (batch) |
| **Internet Banking Service Provider** | Third Party Internet Banking Service Provider | Core Share & Loan Service Provider | Core Share & Loan Service Provider |
| **Website Hosting** | Credit Union | Third-Party Internet Service Provider | Core Share & Loan Service Provider |
| **Credit Union's Connection to Internet Banking Service Provider** | Dedicated Telecommunication Line | Virtual Private Network | Dial-Up |

Unfortunately, there is no silver-bullet solution to address the risks related to e-Commerce. As the table above evidences, the environments used to offer e-Commerce can vary significantly – even among credit unions offering similar services and sometimes even among credit unions utilizing the same service provider(s). Thus, it is critical for each credit union to perform a risk assessment based on its particular environment in order to develop appropriate risk mitigation strategies.

# 6. SECURITY PROGRAM

As a result of performing the risk assessment process, management can identify the impact and likelihood of various threats. Management can then assess the current control structure to determine which controls need to be enhanced and which need to be added in order to bring the risk to an acceptable level. Management should then implement the necessary control policies and procedures to set acceptable risk limits. This will form the basis of the credit union's information security program.

Credit unions are required to have a written security program per Part 748 of NCUA Rules and Regulations. NCUA's security program requirements apply to both the *physical* and *electronic* (or "logical") environments of the credit union. Among other requirements, the security program should be designed to:

- ensure the security and confidentiality of member records;
- protect against anticipated threats or hazards;
- protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member; and
- assist in the identification of persons who commit or attempt such actions and crimes.

Each federally insured credit union files with the NCUA regional director, an annual statement certifying its compliance with the requirements of Part 748. The statement is contained on the Report of Officials that is submitted annually.

The credit union must be able to demonstrate it has an effective program in place that meets regulatory requirements. This provides a flexible approach for developing security programs that are appropriate - given a credit union's unique physical and electronic environment. Examiners may review the credit unions' written security programs during examinations.

In order to assist credit unions in developing and implementing appropriate security programs, NCUA recommends a process that includes the following six key elements:

1. **Involvement of the Board of Directors**

   The board of directors, or its designated committee, should approve the credit union's written information security policy and program as well as maintain oversight over the program.

   Where practical, the credit union should establish a committee or team assigned with the responsibility of developing, implementing, monitoring, and revising security policies and procedures. The team should include representatives from all functional areas of the credit union to ensure input from different perspectives and the development of effective policies and procedures.

   Refer to Chapter 4 of this guide for additional information on oversight of e-Commerce.

**2. Assessment of Risk**

An on-going process is needed to identify risks to member information and information systems, assess likelihood and potential damage of the threats, and assess sufficiency of controls (including policies and procedures) currently in place.

Refer to Chapter 5 of this guide for more information on risk assessment.

**3. Management of Risk**

The credit union should adopt controls that are appropriate given the complexity and scope of the credit union's activities.

Refer to Chapter 5 of this guide for more information on risk management.

Refer to Appendix C for some examples of security control considerations.

**4. Oversight of Service Providers**

The credit union should exercise appropriate due diligence in selecting service providers. Contractual provisions should require service providers to implement and maintain adequate security measures. Credit union management should understand that although services may be outsourced, it is still responsible for ensuring adequate controls are in place to protect credit union and member data.

Refer to Chapter 11 of this guide for more information on service provider oversight.

**5. Adjustments to the Security Program**

The credit union should make the necessary changes to the security program in light of relevant changes in technology, sensitivity of member information, internal or external threats, results of independent assessments, regulatory requirements, and the credit union's changing business arrangements.

**6. Board Reporting**

The credit union should report to the board of directors or appropriate committee at least annually on the overall status of the information security program, including:

- compliance with the program;
- risk assessment;
- risk mitigation;
- service provider arrangements;
- testing results and related action plans;
- security breaches and management's response; and
- recommendations for changes in the information security program.

# 7. PHYSICAL SECURITY ANALOGY

This chapter emphasizes key concepts regarding the protection of member data and draws parallels to threats and control processes credit unions already have in place for protection of physical credit union assets (staff, members, cash, etc.). Poor information security could have consequences as serious, or more serious, than poor physical security.

**Security Measures Vary**

Credit unions are responsible for determining the appropriate security measures for their branches. This results in security measures that can vary widely among credit unions. For example, some credit unions may simply have locks on windows and doors, while others also employ steel bars on windows, motion detectors, video surveillance cameras, bulletproof partitions at teller stations, security guards, etc.

The likely reason for the differences in security measures among branches is the difference in risk levels identified by the credit unions for the unique environment in which their branches operate. The branch environment is comprised of many factors including: location of the branch (e.g., in sponsor's facility), history (e.g., number and type of previous robbery attempts), and services offered at the branch (e.g., cash operations), credit union resource commitment (e.g., financial resources available and dedicated for branch security), etc.

Credit unions are also responsible for determining the appropriate security measures to protect member information systems. This results in security measures that vary among credit unions. The reason for the difference in security measures is the difference in risk identified by the credit union for the unique environment in which it offers e-Commerce. The e-Commerce environment is comprised of many factors including: services offered, outside connectivity, use of outsourcing, type of system used, credit union's network architecture, service provider's network architecture, staff technical expertise, financial resources, physical facilities, existing controls, etc.

**Layered Security Approach**

Effective physical branch security may not rely on one specific security control measure (e.g., lock on doors), but rather a program of many layers of control. For example, if a burglar picks the lock on the front door, he may still have to defeat the front door alarm sensor, then the motion detector, then the vault door (which may have an alarm, a combination, and a time lock, etc.), defeat the locks on the cash boxes in the safe, and then still have dye packs and bait money, and video camera issues to overcome.

Similarly, effective security over member information systems is also not one specific security control, but rather a program of many layers of control. For example, if hackers get past a firewall, they may face authentication controls and encrypted files, all while trying to avoid a detection system.

Unfortunately, many controls have inherent weaknesses and limitations and may be subject to defeat or circumvention. However, it is the cumulative effect of a system of controls that provides the basis for protection that is much stronger than any single control.

## Circumvention of Security Measures

Creative minds can sometimes find ways to bypass many of the layers of security. Examples might include a criminal who tunnels in to the vault from underground, bypassing alarms, doors, etc., or one who gets hired as a branch employee with access to the vault when many security measures (i.e., locks, alarms, etc.) are disabled during working hours.

Similarly, hackers can find ways to bypass layers of security if the credit union is not careful. Circumstances that could permit a circumvention of otherwise good controls include:

- default passwords are not changed on installed system components;
- new vulnerabilities are not identified and patched timely;
- poor password controls are in effect;
- active dial-in modems are present on the network;
- employee system access is not terminated when employment ceases;
- employees are not subject to appropriate background checks;
- employees are not trained to recognize "social engineering" attempts;
- security measures are relaxed during brief maintenance periods;
- access to the physical computer system is not restricted;
- virus software is not updated timely; and
- audit logs are not reviewed on a timely basis for suspicious activity.

Additionally, just as a surveillance camera cannot record important evidence regarding a robbery unless its videocassette recorder is turned on, the system cannot record important evidence regarding an electronic intrusion unless the auditing features are turned on.

## Planning for Foreseeable Security Events

Despite taking what credit unions determine to be reasonable security precautions for their branches, credit unions also develop plans on how to respond to robberies. For example, they have procedures and periodic training on how to react during and immediately after robberies to minimize losses, preserve evidence, and deal with members.

Similarly, plans should be developed to deal with electronic security incidents. Once a security incident is discovered, employees should know what process should be followed to limit losses, preserve evidence, and deal with members.

## Leverage Existing Security Concepts

The above analogies are intended to show that credit unions may be able to leverage existing risk control concepts from their physical environments and apply them to their electronic environments.

# 8. COMMON SECURITY MISCONCEPTIONS

The following two statements are frequent misconceptions regarding security:

1. ***"My credit union only has an informational website, so security is not a concern."***

   If the credit union's site is hosted on the credit union's internal network, then the credit union's member information system may be vulnerable to hackers and viruses.

   Even if the site is not hosted on the credit union's internal network, a hacker "defacement" of the informational website (e.g., posting inappropriate language or pictures) may cause serious reputation issues for the credit union. First, members may take offense to the content. Secondly, members may perceive that the credit union's computer systems have been compromised. This may lead to a loss of trust by the membership. It could also significantly reduce the adoption rate of any future interactive or transactional website iterations that may be in development or planned.

   In fact, even a credit union without a website can face threats from hackers and viruses. Some credit unions have an "always-on" cable or DSL (Digital Subscriber Line) Internet connection (sometimes called "broadband"). Such credit unions may use this Internet access solely for e-mail and web browsing. Since these connections have a "static" Internet address that does not change, it provides an easy way for a hacker to return to the credit union. Additionally, since these connections are "always-on," they may provide gateways to gain access to the credit union's systems at any time.

   Furthermore, even a credit union with a "dial-up" Internet connection faces some risk. For instance, viruses can be encountered by simply accessing websites, downloading files from websites, opening files in e-mail messages, etc. In fact, vulnerabilities have even been discovered in the use of Internet instant messaging programs that could compromise system security.

2. ***"A firewall is all that is needed for strong security."***

   A firewall may be part of a system of controls, but it is only one part. There are several different types of firewalls, each with their distinct advantages. If a firewall is not configured properly it will not provide adequate security. If the firewall logs are not monitored and responded to in a timely manner, suspicious activity may go undetected. There may be numerous other ways to gain access to member information systems (or Internet banking services) that are not dependent on defeating a firewall (e.g., dial-up modem on the network behind the firewall, disgruntled ex-employees with remote system access that is still active, poor authentication process, poor controls over passwords, etc.).

It is only with a thorough and on-going risk assessment process, based on the credit union's unique e-Commerce environment (i.e., services offered, outside connectivity, use of outsourcing, type of system used, credit union's network architecture, service provider's network architecture, staff technical expertise, financial resources, physical facilities, existing controls, etc.), that appropriate control measures can be determined.

# 9. LEGAL & REGULATORY COMPLIANCE CONSIDERATIONS

Credit unions should understand that many of the traditional compliance issues also apply to e-Commerce, including:

- Equal credit opportunity;
- Electronic funds transfer;
- Expedited funds availability;
- Fair credit reporting;
- Fair housing;
- Real estate settlement and procedures;
- Right to financial privacy;
- Truth in lending;
- Truth in savings;
- Nondiscrimination;
- Advertising;
- Bank secrecy; and
- Suspicious Activity Report (SAR) filing.

Additionally, laws are now in place addressing privacy, electronic signatures, and security that may impact e-Commerce initiatives.

In those instances where e-Commerce is evolving more rapidly than legal standards and remedies (i.e., lack of related case law), legal counsel should address the credit union's procedures and practices for ensuring that e-Commerce transactions are legally binding.

A process should be in place to ensure the credit union is aware of, and has addressed all relevant legal and compliance issues regarding e-Commerce. Therefore, it is prudent to involve legal counsel in the review of e-Commerce initiatives. If the legal counsel historically utilized by the credit union is unfamiliar with e-Commerce related issues, they may be able to refer the credit union to counsel with such expertise.

Some areas that would typically warrant review to facilitate compliance with applicable laws, regulations, prescribed practices, and ethical standards may include:

- contracts;
- website content (including links to other sites);
- e-Commerce insurance;
- new products and services; and
- policies and procedures.

Legal counsel (and credit union compliance staff) will likely play a key role in the on-going risk assessment and mitigation process of the credit union for e-Commerce.

# 10. INDEPENDENT ASSESSMENTS

One method of validating the credit union's risk control measures for e-Commerce activities is through independent assessments. There are no current regulatory requirements for independent assessments of credit union e-Commerce systems. Credit union officials must exercise judgment, based on the results of the risk assessment process, in deciding which, if any, assessments to have performed on their e-Commerce environments.

Terminology and scopes for assessment services vary. The key is to understand the specific scope and methodology for a particular assessment. For example, some assessments are limited to a review of system documentation to assess potential network vulnerabilities, while others may involve an "attack" on the credit union's systems. Some may even involve attempted physical access to systems, or social engineering. Still others, may strictly involve a review of the website for compliance issues.

Factors management should consider when contracting for third-party assessments include:

- **Scope** – What is specifically subject to review and what is specifically excluded from the review?
- **Methodology** – What specific procedures (e.g., network scanning, social engineering, network penetration, etc.) will be performed and what specific procedures are not permitted (e.g., changes to system, financial transactions, etc.)?
- **Timing** – When, and how frequently, will the assessment be performed?
- **Involvement** – Will the assessment be announced in advance to all key parties, or just certain management and staff?
- **Qualifications** – What is the reputation, training, experience, and applicable certification of the specific people who will be performing the assessment?
- **Background Checks** – Are the assessment organization's staff bonded and subject to background checks?
- **Contract** – Is the work to be performed outlined in writing, along with appropriate review by legal counsel? Are privacy, confidentiality, and other provisions addressed in the contract?
- **Information Provided** – What information will be provided (e.g., credit union's modem phone numbers, names and versions of critical system components, etc.) to assist the third-party, and what will not be provided (e.g., passwords, system configuration, etc.)?[1]
- **Results** – When, in what detail, and in what format will the report or certification be delivered? Will copies of the results also be maintained by the third-party? If so, for how long, and under what protective measures?
- **Ownership** – Who (e.g., supervisory or audit committee, e-Commerce committee, information systems management, security officer, etc.) is responsible for the relationship with the third-party?

[1]This will vary depending on the scope of the evaluation. For instance, if a penetration test is planned, the test can be designed to simulate a penetration attempt by someone with no knowledge of the organization's environment or it can be designed to simulate a penetration by someone with "inside" information. Many security breaches are credited to insiders (or insider assistance). The credit union's risk assessment should assist in determining the extent and type of information provided.

Credit unions should understand that there might be a lack of industry standards for some types of assessments and some assessments could lead to inadvertent damage to credit union data and systems. Credit unions should consider issuing a Request for Proposal (RFP) that outlines the requirements for the assessment it wants to outsource. The factors noted above may be appropriate for inclusion in the RFP and facilitate an effective comparison of assessment providers.

## Assessment Results

The results of internal and external assessments should be communicated in written form to the credit union. The issues raised in the report should be ranked in order of importance based on potential impact to the credit union. Planned corrective actions should be determined for all issues. This information should be reported to senior management, the board of directors, and the supervisory or audit committee.

Assessment reports should be handled with care. For example, some may detail security vulnerabilities of the credit union's systems. If that information was to reach the public domain, it could potentially cause the credit union harm.

Periodic updates should be provided to the board of directors on the progress of the planned corrective actions. The supervisory or audit committee, or its internal auditors, should follow-up to ensure corrective action has been taken.

Credit unions should understand that the assessment results are as of a specific point in time. Changes in the credit union's environment (i.e., services offered, outside connectivity, use of outsourcing, type of system used, credit union's network architecture, service provider's network architecture, staff technical expertise, financial resources, physical facilities, existing controls, etc.), as well as changes in the threat environment (e.g., new hacking tools, discovery of new system vulnerabilities, etc.), or a breakdown in controls (e.g., untimely system patches and updates, etc.) could significantly impact the credit union's risk exposure at any time.

## Other Sources of Independent Assessments

The supervisory or audit committee, or its internal auditors, may also perform certain independent reviews. The type and extent of their reviews will vary depending on their skill sets and resources. Additionally, in some instances, the credit union's insurance company may offer a complimentary limited assessment of the credit union's e-Commerce control environment.

## Service Provider Assessments

In addition to independent assessments of credit union operations, independent assessments of service providers may also provide important information for credit union officials responsible for managing the risks associated with e-Commerce.

There are no regulatory requirements for independent assessments of the operations of third-party service providers. Thus, if the credit union's risk assessment process points to a need for independent assessments of its service providers, this should be specifically addressed in the contract with the service provider.

Some service providers may not agree to have an independent assessment performed on their operations – regardless of who bears the cost.

Some service providers who do have independent assessments may be unwilling to share the detailed results of certain types of third-party assessments performed (e.g., network scans, vulnerability assessments, penetration tests, etc.) due to security concerns. Although, some may be willing to share high-level results and discuss the types of assessments the organization receives and how it reacts to them.

Some service providers may also obtain independent certifications to evidence that their practices regarding security and/or privacy are adequate. Credit unions are encouraged to review the certification organization's requirements to determine if the certification appropriately addresses the credit union's concerns.

Some service providers may obtain a Statement of Auditing Standards (SAS) 70 review, "Reports on the Processing of Transactions by Service Organizations." This report is the result of an independent review and is intended for the financial auditors of the service provider's clients. A SAS 70 Type I report will describe the controls at the service provider at a point in time. A SAS 70 Type II report is based on actual testing of controls over a given period of time (generally six months) at the service provider. Both reports may contain user considerations for controls that may be needed at the credit union. Credit unions should understand that the SAS 70 report does not provide an opinion on e-Commerce security or disaster recovery.

If a report on a service provider is obtained, the credit union should review it and follow up on any concerns or outstanding control issues with the service provider – as well as consider what, if any, additional controls may be needed at the credit union based on the report.

# 11. EFFECTIVE MANAGEMENT OF THIRD-PARTY RELATIONSHIPS

Credit unions are becoming increasingly reliant on third parties to support information technology (IT) services, including e-Commerce initiatives. Officials who outsource IT services generally do so to manage cost, provide information technology expertise (not available in-house), and to expand and improve product and service offerings to their members.

**The use of third parties does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner, and in compliance with applicable laws**. Thus, an effective due diligence process and on-going oversight process are critical to the effective management of third-party relationships. Specifically, the credit union should have a process in place to:

- assess how outsourcing arrangements will support the credit union's objectives and strategic plans;
- understand the risks associated with outsourcing arrangements for technology services;
- ensure appropriate contractual provisions are in place to facilitate effective oversight; and
- implement an oversight program to monitor each service provider's controls, conditions and performance.

Each of these steps will be discussed in more detail below.

## Assessing Outsourcing Arrangements

Prior to entering into outsourcing arrangements, credit union management should perform a requirements analysis to identify the credit union's specific needs. The analysis should address:

- level of services and/or support required;
- functionality and capacity required; and
- system performance requirements.

Management should consider developing and distributing a Request for Proposal (RFP) to solicit responses from potential service providers. The RFP should address specific requirements and request qualifications and references, as well as fee estimates or caps. By issuing an RFP and soliciting responses, management will be better able to obtain and review multiple bids from service providers, rule out unacceptable responses, and identify the best-qualified providers.

## Understanding Risks

Effective service provider risk assessment practices include determining the:

- credit union's ability to evaluate and oversee outsourcing relationship;
- importance and criticality of services provided;
- requirements for outsourced activity;
- contractual obligations and requirements for the service provider, including independent validation/certification of service provider's control environment and financial condition, and escrowing of e-Commerce software code;

- service provider and credit union responsibilities for security, privacy and regulatory compliance and guidance for affected parties; and
- contingency plans, including availability of alternative service providers, costs and resources required to switch service providers.

## Contractual Considerations

Management should periodically evaluate service providers to determine their ability, both operationally and financially, to meet the credit union needs. One of the most effective ways to address and manage risk is to ensure the contract between the credit union and the service provider is clearly written and sufficiently detailed to provide assurances for performance (operational, financial, and system), reliability, security, privacy, ownership of data, disaster recovery capabilities, and reporting (e.g., performance, audited financial reports, security evaluation summaries, security incidents impacting the credit union, etc.). Specific service level agreements (SLAs) tied to specific actions (e.g., price concessions, early contract termination rights, etc.) should be considered to protect the credit union.

The contract should address business requirements and key factors identified during the risk assessment and due diligence phases – such as the availability of audited financial reports (especially for private companies), reports on the internal control environment (SAS 70), any other reports (e.g., high-level summaries of security assessments), and appropriate security measures to be deployed (e.g., firewalls, intrusion detection, background checks and bonding of service provider employees, etc.). The contract should also be flexible enough to allow for changes in technology, strategic initiatives and operations. Appropriate legal counsel should review contracts prior to execution.

A credit union may find it beneficial to establish similar contract expiration time frames for all e-Commerce related activities and its core share and loan arrangements, to facilitate transitioning to different service provider(s) if the need arises.

## Oversight Program

Credit unions should implement an oversight program to monitor each service provider's controls, conditions and performance. This oversight program should:

- clearly assign responsibility for the administration of each service provider relationship;

- ensure the level of effort (e.g., number of personnel assigned, functional responsibilities, and amount of time needed) to monitor service provider correlates with the scope, complexity, and risk relative to the services provided; and

- set standards for the maintenance of documentation to be used for contract negotiations, termination issues, and contingency planning.

# 12. BUSINESS CONTINUITY

Each credit union should determine the importance of e-Commerce services to its operations. The credit union's tolerance for a lack of such services in the event of a disruption (e.g., equipment malfunction, business failure of service provider, local disaster, security incident, etc.), will dictate the resources to be dedicated to business continuity for e-Commerce.

Factors that may impact the criticality of e-Commerce include:

- role of e-Commerce in the credit union's strategic plan;
- scope of e-Commerce offerings (e.g., transactional capabilities, bill payment, etc.);
- adoption rate (e.g., member usage, including transaction volume) of e-Commerce;
- member expectations and perceptions regarding the availability of e-Commerce services; and
- availability of other delivery channels (e.g., ATM, audio response, branches, etc.) to conduct business in the event of a business interruption.

For some credit unions, a short-term interruption may pose an unacceptable risk. Yet for other credit unions, a long-term interruption may pose a minimal risk. The criticality of e-Commerce availability will vary among credit unions and so will their resulting business continuity plans.

As the reliance on e-Commerce is likely to change over time, management should periodically reassess the criticality of e-Commerce to its operations to ensure the appropriate resource level is committed for e-Commerce business continuity.

Business continuity plans should be based on a risk assessment that identifies and prioritizes critical systems, based on their impact on the organization in the event of various disruption scenarios. Responsibilities, actions, time frames, and notifications should be detailed in the plan.

Daily back-up procedures should support the recovery plan for e-Commerce. The current version of the website and the configurations for key network components (e.g., firewalls) should be subject to back-up procedures. This information should be kept to facilitate timely reestablishment of the website (with an acceptable level of security) under certain business disruption scenarios, and to assist with forensic evidence if a crime was committed. Consideration should also be given to the amount of time backups are kept for logs, as system intrusions may go undetected for significant periods of time.

Business continuity plans should be updated (based on new service offerings, new network components, new service providers, etc.) frequently and tested at least annually. To the extent that service providers are utilized, testing should be coordinated to ensure the viability of the plans. Results of the test and planned corrective actions should be communicated to senior management, the board of directors, and the supervisory or audit committee.

# 13. MEMBER SERVICE

Credit unions should have a defined process to address member inquiries related to e-Commerce. Member service representatives should receive periodic training to ensure their skill levels are commensurate with their responsibilities related to e-Commerce.

Credit unions may choose to implement a process to track member service inquiries that allows for prioritization of the calls, reporting of open items, and the time frame from initial contact to final resolution of each inquiry. Tracking the type of member support issues related to the e-Commerce site may prove helpful in:

- development of "frequently asked questions" (FAQs) posted to the website;
- future improvements to the site or services; and
- training of member service representatives.

Procedures will likely be needed to assist members who get "locked-out" of their accounts, forgot their personal identification number (PIN), or want to dispute an on-line transaction.

Credit unions that rely on third-party service providers to deliver their e-Commerce solutions, may consider the need to use contractual service level agreements that outline penalties for not meeting the requisite level of performance (e.g., system availability).

A credit union should pre-determine the type and detail of information it will share with inquiring members regarding its security measures. Too little information may cause members to shy away from using the credit union's e-Commerce services. Too much detail could compromise the credit union's security. Member service representatives should understand how to handle such inquiries. Furthermore, the credit union should consider addressing security in the FAQ section of the website.

Members may also look to the credit union for guidance on how to protect themselves when using the Internet (e.g., firewalls, virus protection, latest versions of browsers, etc.). Links to other websites (e.g., security organizations, consumer organizations, government consumer agencies, law enforcement agencies, etc.) and FAQs may be helpful in these cases.

Consideration should be given to contacting members who are locked out of their accounts. The credit union can provide assistance in reestablishing access. This is also a good way to identify accounts that may be subject to unauthorized attempted access.

Consideration should also be given to tracking the number of members who stop using e-Commerce services. A survey could be done to assist in determining the primary reasons for attrition. Modifications to the website may be made based on such feedback to attract and retain users.

# 14. PERFORMANCE MONITORING

## Website Monitoring

Website availability may be critical to the success of a credit union's e-Commerce service offerings. Automated tools are available that will allow credit unions to monitor the availability of their websites. Tracking this information will enable credit unions to respond to unplanned system outages in a timely manner.

Monitoring tools can also determine other key performance measures such as average response times, processor utilization, number of simultaneous sessions, etc. By tracking this type of information, management can anticipate whether the website will be able to handle the desired concurrent usage or whether system performance will be negatively impacted.

## Strategic Measurements

Management should compare actual performance with projections to measure the success of e-Commerce initiatives. Performance criteria for a credit union's website may be based upon long-term and/or short-term plans and goals, or member expectations and demands. For example, if a credit union's strategic goal is to have a certain number of members actively using e-Commerce by a specific date, management will likely want to monitor and periodically report the number of unique user "logons" to the board of directors on a periodic basis.

When actual performance falls short of targeted goals, a credit union may wish to consider additional actions to achieve their goals. For instance, if the number of members actively using Internet banking is low, perhaps additional marketing efforts are needed, or the website's frequently asked question (FAQ) section may need to be expanded, or a survey should be conducted of those members who stopped using the service to determine the specific reasons, etc.

# 15. SUMMARY

Part 721 of NCUA's Rules and Regulations identifies activities deemed to be within the incidental powers of a federal credit union. Electronic financial services are included in such services. Additionally, Part 748 of NCUA's Rules and Regulations requires federally-insured credit unions to develop a written security program to protect the security of member data.

As such, NCUA encourages credit unions to evaluate if e-Commerce is a good fit for their members. e-Commerce is a logical offering for many credit unions. It can provide for increased access to services, as well as new types of services, for credit union members. It may help credit unions to retain and attract members who do not have convenient access to the credit union's branch location(s). However, e-Commerce must be offered in an environment that protects member data and the credit union's hard-earned reputation if the credit union wants to remain its members' primary financial institution.

**Familiar Process**

As with any new product or service, a credit union must do its homework. For instance, regardless of a credit union's size, it should go through a process that includes the following:

- involve all stakeholders in planning and implementation;
- determine member demand;
- seek education about the benefits and risks;
- determine if risks are acceptable and manageable;
- evaluate necessary security measures;
- determine regulatory compliance requirements;
- research available bond and insurance coverage;
- assess the adequacy of staff expertise (technical, managerial, member service);
- train staff, as necessary;
- seek expert assistance, if needed;
- identify the best in-house/outsourcing solution;
- perform due diligence on service providers;
- ensure a legal review of related contracts;
- create or revise related policies and procedures;
- implement appropriate controls; and
- periodically evaluate performance and make changes as necessary.

e-Commerce technology planning is the aggregate process outlined above (and explained in more detail throughout this guide and related issuances). Appropriate planning is critical for successful implementation of e-Commerce in a safe and sound manner.

**A Matter of Trust**

Members trust their credit union to take reasonable precautions to protect financial and personal information. This trust has been earned over many years, but it could be significantly damaged in a short period of time should member information systems be compromised. A credit union must ensure its members' trust is well founded when it comes to the world of e-Commerce.

# APPENDIX A – NCUA Reference Material

| Letter to Credit Unions # | Date Issued | Subject |
|---|---|---|
| 02-FCU-11 | Jul-02 | Tips to Safely Conduct Financial Transactions Over the Internet - Brochure |
| 02-CU-13 | Jul-02 | Vendor Information Systems & Technology Reviews – Summary Results |
| 02-CU-08 | Apr-02 | Account Aggregation Services |
| 02-FCU-04 | Mar-02 | Weblinking Relationships |
| 01-CU-21 | Dec-01 | Disaster Recovery and Business Resumption Contingency Plans |
| 01-CU-20 | Nov-01 | Due Diligence Over Third Party Service Providers |
| 01-CU-12 | Oct-01 | e-Commerce Insurance Considerations |
| 01-CU-09 | Sep-01 | Identity Theft and Pretext Calling |
| 01-CU-11 | Aug-01 | Electronic Data Security Overview |
| 01-CU-10 | Aug-01 | Authentication in an Electronic Banking Environment |
| 01-CU-04 | Mar-01 | Integrating Financial Services and Emerging Technology |
| 01-CU-02 | Feb-01 | Privacy of Consumer Financial Information |
| 00-CU-11 | Dec-00 | Risk Management of Outsourced Technology Services (with Enclosure) |
| 00-CU-07 | Oct-00 | NCUA's Information Systems & Technology Examination Program |
| 00-CU-04 | Jun-00 | Suspicious Activity Reporting (see section regarding Computer Intrusion) |
| 00-CU-02 | May-00 | Identity Theft Prevention |
| 97-CU-5 | Apr-97 | Interagency Statement on Retail On-line PC Banking |
| 97-CU-1 | Jan-97 | Automated Response System Controls |
| 109 | Sep-89 | Information Processing Issues |

| Regulatory Alert # | Date Issued | Subject |
|---|---|---|
| 01- RA-08 | Aug-01 | Interim Final Rules Amending Regulations B, E, M, Z and DD - Electronic Delivery of Required Disclosures |
| 01-RA-07 | Jul-01 | Children's Online Privacy Protection Act (COPPA) |
| 01-RA-03 | Mar-01 | Electronic Signatures in Global and National Commerce Act (E-Sign Act) |
| 99-RA-3 | Feb-99 | Pretext Phone Calling by Account Information Brokers |
| 98-RA-4 | Jul-98 | Interagency Guidance on Electronic Financial Services and Consumer Compliance |

| Rules & Regulation | Date Issued | Subject |
|---|---|---|
| 12 CFR Part 721 | Jul-01 | Federal Credit Union Incidental Powers Activities - Identifies activities deemed to be within the incidental powers of a federal credit union. Electronic Financial Services and Stored Value Products are addressed |
| 12 CFR Part 748 | Jan-01 | Security Program and Appendix A - Guidelines for Safeguarding Member Information |
| 12 CFR Part 716 | Jun-00 | Privacy of Consumer Financial Information |
| 12 CFR Part 741 | May-00 | Requirements for Insurance |

Please refer to NCUA's website (http://www.ncua.gov) for the latest reference material available regarding Information Systems and Technology (IS&T).

# APPENDIX B – Sample List of Policy & Procedure Considerations

There are many possible starting points for policy development, including revise old, develop new, obtain from peer credit unions, purchase templates from third party, develop via consultants, find samples via Internet-based research, etc. Regardless of the starting point, the final policies and procedures must be appropriate for a credit union's unique environment and meet its operational control needs.

The credit union should determine which areas need to be addressed in policies and procedures based on its e-Commerce environment. Some areas may require their own separate policies and procedures, while others may be incorporated in existing policies and procedures. Examples of areas that may need to be addressed in policies and procedures include:

- **e-Commerce** – How does the credit union establish its overall policy for the use, objectives, high-level controls, and oversight of e-Commerce at the credit union? It may reference other applicable policies as needed. Related information appears in Chapter 4.

- **Security Program** – How does the credit union control physical and logical security related to e-Commerce? Related information appears in Chapter 6.

- **Security Awareness Training** – How does the credit union ensure that employees (and possibly members) are aware of the risks of e-Commerce and the security measures that are needed for protection? Related information appears in Appendix C.

- **Risk Assessment** – How does the credit union identify and manage risks related to e-Commerce? Related information appears in Chapter 5.

- **Data Classification**– How does the credit union classify the sensitivity and criticality of data residing on, or transmitted through, its systems? This will assist in determining appropriate security data protection measures. Related information appears in Chapter 5.

- **Desktop and Laptop Security** - How does the credit union control and protect (e.g., encryption) member data that resides on these machines?

- **Service Provider Due Diligence & Oversight** – How does the credit union manage the selection and on-going oversight of service providers that play key roles in the delivery of e-Commerce services? Related information appears in Chapter 11.

- **Virus Protection and Prevention** – How does the credit union protect its systems against malicious code? Related information appears in Appendix C.

- **Remote Access** – How does the credit union control remote access (i.e., authentication, VPN, use of firewalls and anti-virus software on remote PCs, etc.) to internal systems by its employees and service providers? Related information appears in Appendix C.

- **e-Mail Use** – How does the credit union define and control appropriate e-mail use?

- **Incident Response** – How does the credit union respond to e-Commerce related security incidents? Related information appears in Appendix C.

- **Business Continuity** – How does the credit union respond to interruptions and disasters related to e-Commerce? Procedures should be outlined for system back-ups and may be included or referenced from here. Related information appears in Chapter 12.

- **Board Reporting** – How does management expect to report (format, frequency, etc.) to the board of directors on e-Commerce related activities and security events? Related information appears in Chapters 4, 5, 6, 10, 11, 12 and 14.

- **Wireless Communications** – How does the credit union implement secure wireless networking and/or secure wireless delivery of electronic financial services to members? Related information appears in Appendix C.

- **Third Party Network Connection** – How does the credit union control third-party connectivity to its internal network? Related information appears in Appendix C.

- **Acceptable Use** – How does the credit union define and control appropriate and inappropriate use of its systems by employees?

- **Password Selection and Change**– How does the credit union control passwords for staff and members related to e-Commerce? Related information appears in Appendix C.

- **System Architecture and Controls** – How does the credit union control and document its systems (hardware and software) related to e-Commerce? Related information appears in Appendix C.

- **System Development and Acquisition** – How does the credit union control the development or purchase of hardware and software related to e-Commerce?

- **Configuration, Monitoring, and Maintenance** – How does the credit union manage the set up, monitoring, and maintenance of infrastructure components (e.g., host, router, firewall, etc.) that are critical to the secure delivery of e-Commerce services? This may include the audit policy that defines the type of security events that are logged. Related information appears in Appendix C.

- **External Consulting Services** – How does the credit union utilize third-party experts for assessing security related to e-Commerce? Related information appears in Chapter 10.

- **Member Support** – How does the credit union manage member service related to e-Commerce activities? Related information appears in Chapter 13.

- **Personnel Hiring & Termination** – How does the credit union manage access (physical and logical) for new, promoted, and terminated employees? Related information appears in Appendix C.

# Appendix C – Security Control Considerations

Credit unions must keep abreast of the rapidly changing e-commerce environment in order to make informed judgments in order to reduce risks to an acceptable level.

There are many sources of information on e-Commerce threats and control measures, including: the credit union industry (e.g., websites, periodicals, reports, meetings, on-line forums, etc.), bonding companies, security organizations (e.g., websites, periodicals, training sessions, etc.), auditors, expert consultants, peer credit unions, and regulators (e.g., issuances, websites, examiners, etc.).

Each credit union should adopt the necessary controls to protect member information systems as it deems necessary based on a thorough risk assessment (based on its unique environment for offering e-Commerce). Without a thorough risk assessment, a credit union might find itself in a situation that exposes itself and its members to a higher level of risk than would otherwise be acceptable. For example, without a strong authentication process, a credit union could find itself in the following hypothetical situation:

1. A member pays for a purchase (e.g., buys flowers) using a share draft.

2. The receiver of the share draft (e.g., store clerk) notes key information from the share draft (e.g., credit union's name, member's name, member's social security number, member's account number).

3. The clerk enters the credit union's name into an Internet search engine to locate the credit union's website.

4. The clerk uses the member's account number and social security number (or last four digits) to access the member's account on-line. This would be possible if the credit union relied solely on these two pieces of public information to: (a) sign-up for Internet banking access, or (b) gain access to accounts already signed-up for Internet banking access.

5. The clerk would then have the same level of access as the member (including possibly accessing the member's joint accounts). Depending on the type of e-Commerce services offered, the clerk may be able to: change the address of the member, transfer funds among accounts, have a check disbursed, draw on a line of credit, apply for a loan, order additional checks, possibly alter electronic bill payments, etc.

This appendix will outline the following control considerations:

I. Personnel
II. System Architecture
III. Physical Control
IV. Logical Access
V. System Maintenance
VI. System Monitoring and Incident Response
VII. Security Program Validation
VIII. Outsourcing

## I. Personnel Considerations

The credit union's staff is its primary asset in protecting member information. The effectiveness of robust security policies and systems are severely diminished if personnel do not understand and implement them appropriately. Additionally, credit union staff may be in the best position to circumvent controls. Therefore, basic controls, training, system access, and retention should be considered critical control areas warranting close scrutiny. Key considerations include:

### Basic Control Measures

As with other areas of credit union operations, the following should be in place to reduce the threat of fraud, misconduct, or staff unavailability related to e-Commerce:

- **segregation of duties** (e.g., employee that initiates changes to the website, should be different than the employee who approves and releases the changes, etc.);

- **dual control** (e.g., access to critical system passwords in case of an unplanned departure of key employee responsible for information systems, etc.); and

- **cross-training** (e.g., installing software patches, reviewing firewall reports, etc.).

### Training

On-going security awareness training should be provided to all employees to ensure they understand their responsibilities related to the credit union's information security program. Training should include awareness of techniques such as "social engineering" used by criminals to gain important information for use in breaching security.

Technical training should be given to those employees responsible for technical aspects of security (e.g., firewalls, intrusion detection, security policy development, etc.).

### System Access

Staff with access to member information systems should be subject to appropriate background checks (e.g., employment verification, criminal check, credit check, etc.) determined by the credit union. Furthermore, controls should be in place to provide reasonable assurance that system access for employees is commensurate with current job responsibilities, and system access is removed expeditiously when employment is terminated.

### IT Staff Retention

If the credit union is large enough to support a professional IT staff, then it should consider a plan for the recruitment, retention, and cross-training of skilled IT professionals to minimize the security (and operational) impact of the loss of a key IT employee.

## II. System Architecture Considerations

The credit union's information system infrastructure should be designed for reliability and to protect member data from unauthorized access. Management should maintain an updated inventory of all hardware and software, as well as diagrams showing the design and connectivity of the network components. Key considerations include:

**Network Design and Configuration**

- implementing internal or external redundancy to ensure continued operation in the event a component fails or is shut down for maintenance;
- designing a network that is scalable to accommodate growth and has interoperability with existing and planned systems;
- using firewalls to filter all traffic (including service providers) to/from (via Internet, dedicated telecommunication line, etc.) the credit union's internal network;[1]
- using an intrusion detection system ("IDS") to detect potentially harmful network activity;[2]
- using a virus protection mechanism to protect the system from harmful hidden code ("programs") that can cause harm (e.g., destroy data, use all the system resources, launch attacks on other systems, overwhelm the e-mail system, etc.) to the credit union's information system;[3]
- implementing a "demilitarized zone" (DMZ) design to the network;[4]
- utilizing separate servers for critical functions (e-mail, website, production, etc.);[5]

[1] There are different types of firewalls, each with its own pros and cons. Some sophisticated organizations implement different types of firewalls on their network as a strategy to "buy time" if a hacker defeats one type of firewall. Firewalls should be designed to disallow all traffic if they fail versus passing all traffic through to the internal network. Some firewalls are software, while others are a combination of software and hardware.

[2] There are different types of IDS (e.g., host-based, network-based) and functionality levels (e.g., "real-time" alerts, automated response, etc.) of intrusion detection systems.

[3] There are different ways to implement and manage virus protection for a computer network. Regardless of the approach implemented by the credit union, it is critical to ensure the software is updated (with virus "definitions") in a timely manner to ensure protection from the latest viruses.

[4] This design strategy separates the internal network components (e.g., computer with member information database) from the network components with external connectivity (e.g., Web server). While DMZ design may vary, firewalls are critical components used to achieve the desired level of separation.

[5] This design practice facilitates security, availability of services, and efficiency. By using separate machines, the impact of one machine being compromised may be less because not all services are on that machine, the impact of one machine failing is not as great because other services can continue, and the machine will be more efficient as it can be configured to best perform for the single task it is assigned.

- limiting and protecting sensitive information stored on the web server;[6] and

- ensuring good "auditability" by activating audit logs for various components to ensure a record exists to assist forensic experts trying to trace inappropriate activity (e.g., hackers).[7]

**Network Diagrams**

Diagrams may vary in the level of detail but, at a minimum, should depict all system components and their connectivity (internal and external). They are important for the risk assessment process because they assist in identifying vulnerability points (external connectivity) and potentially poor system design (e.g., lack of firewalls or lack of demilitarized zones). Network diagrams should be considered sensitive information and care should be taken with their storage and distribution.

**Network Inventory Listing**

This list should include hardware and software. Operating systems, versions, patches, etc. should be documented. Availability of this documentation is likely to prove beneficial for:

- familiarizing new staff with the information system;
- determining what systems may need security patches;
- converting or upgrading components of the system;
- completing security assessments;
- planning and implementing business recovery procedures;
- ensuring compliance with software licenses;
- implementing certain protection systems (e.g., intrusion detection, virus protection, etc.);
- completing insurance claims; and
- recording credit union assets for accounting purposes.

## III. Physical Control Considerations

Critical data processing equipment should be maintained in a physically secure environment to reduce the likelihood of environmental damage or inappropriate access to member information systems by employees, contractors, service providers, members, and others. Key considerations include:

- **access control devices** - (e.g., physical locks, magnetic keycard readers, biometric readers, etc.) and the granting of access based on specific responsibilities (and removing such access immediately upon termination of relationship);

[6] The Web server is more vulnerable than other parts of the credit union's network because of its necessary exposure to the Internet. All data stored on the Web server should be carefully evaluated to determine the appropriateness of it being stored there (e.g., member data, passwords, etc.) and the level of protection (e.g., encryption) afforded to such data that is stored there.

[7] Credit unions should consider using media that writes only one time (vs. the ability to write over existing data) to avoid clever hackers who try to alter audit logs to hide their tracks.

- **monitoring systems** - alarms (e.g., burglar and fire, monitored or unmonitored, etc.);

- **protection systems** - fire suppression systems (e.g., manual or automated extinguisher system, etc.); and

- **component location –** ideally computer equipment should be placed in areas of the facility that are less likely to be subject to the impact of flooding. Consideration should be given to placing the equipment on raised platforms or enclosed equipment racks or other means (e.g., tarps) to protect from damage from certain types of fire suppression systems.

## IV. Logical Access Considerations

Logical (electronic) access to member information systems should be restricted and monitored to reduce the likelihood of damage or inappropriate access to member information systems. It is understood that equipment and options for protection may vary significantly among credit unions. Key considerations when evaluating logical access include:

**Enterprise-wide Considerations**

- Identification of all parties accessing credit union systems (e.g., staff, service providers, contractors, members, etc.);

- Identification of all logical access methods (e.g., internal workstations on the network or remote access via Internet, dial-in to modem, wireless, dedicated telecommunication line, etc.);

- Identification of the network connection location for each of the parties and methods noted above (e.g., direct-dial into modem built-in to the production server, connections to the internal network behind the Internet firewall, Internet connection, etc.); and

- Determination of appropriate controls (e.g., authorization for access, authentication procedures, time of day access controls for certain staff, encryption, virus protection, firewall, manual activation of modem, etc.) used for each type of connection and based the user's authorization level (via the system policy) for access to member information systems.

If separate systems are used for testing, and those systems have actual member information (even if the information is old), these systems should also be subject to appropriate physical and logical controls.

**Internet Banking Considerations**

- The credit union should implement strong authentication procedures for initial account enrollment and subsequent account access.

    a. Does the credit union require initial passwords that are randomly generated by the system or allow passwords based on information that is likely available to the public (e.g., social security number)? Note, the use of a secondary PIN may also be a consideration and impact such decisions.

    b. Does the credit union require (to the extent possible), rather than request, strong password selection and change controls such as:

        - Passwords cannot be the member's name, social security number, account number, phone number, previously used passwords, etc.
        - Passwords must be of a certain character length (e.g., seven characters) and composed of certain types of characters (upper case letters, lower case letters, numbers, special characters, etc.).
        - Password expirations/required changes after a predetermined period of time. If the credit union's automated response processing system will not mandate password changes, the credit union should consider warning members of the inherent risks of not making the change.

    c. Does the credit union require appropriate security measures over the delivery of initial passwords to members?

    d. Does the credit union require an account to be active (i.e., not dormant) in order to be eligible for Internet banking services?

    e. Does the credit union determine if dollar limits (per transaction and/or daily aggregate) should be established for on-line transactions?

- The credit union should implement controls to block Internet banking access after a limited number of failed authentication attempts. The credit union should determine:

    a. The number of failed logons (e.g., 3 attempts) prior to locking the Internet banking access.
    b. The means (e.g., call in to the credit union for verbal authentication and manual reset, an automated reset of blocked accounts after 10 minutes, etc.) by which a blocked account is reactivated for potential Internet access.
    c. What, if any, notification (e.g., e-mail, letter, phone call) to the member when their account is locked out due to failed login attempts.
    d. What, if any, reporting/tracking of such instances is needed by the credit union.

- The credit union should implement controls to end an Internet banking session based on:

    a. The time period (e.g., number of minutes) after which an Internet banking session is terminated due to lack of activity.

b. The time period for which an active Internet banking session is permitted to remain open (regardless of activity).

- The credit union should implement controls to control web page "caching" so unauthorized individuals cannot use the "back" command for the Internet browser to view or gain electronic access to a member's account.

- The credit union should implement controls to protect member data transmissions. Credit unions should consider:

    a. Restricting Internet banking services only to those members using a web browser with an appropriate encryption capability. Browser upgrades are available via the Internet at no cost. Note, although many credit unions currently support 128-bit SSL for Internet banking, they may also be permitting sessions at 56-bit encryption (which provides a much lower level of security).

    b. Encrypting wireless network transmissions and highly sensitive data in storage (this may add a critical level of protection if other security measures are defeated).

- The credit union should implement controls to protect the credit union's Internet address to reduce the likelihood of members being lured to an imposter site used to fraudulently obtain member information (passwords, etc.). Methods include:

    a. Registering similar domain names including formal names and acronyms, as well as different neighborhoods (suffixes) such as ".com," ".org," ".net," ".coop," etc. to avoid confusion and prevent fraud.

    b. Communicating domain name registration changes to the registrar in a manner that ensures a high degree of certainty that the credit union (versus an imposter) authorized the changes. This can include callback procedures, passwords, etc.

    c. Using a secure server identification certificate to protect communications between the server and website visitors. This will encrypt the communication sessions and also allow for authentication that the website is that of the credit union.

    d. Reviewing the updated guidance available from the domain name registration organization and encryption certificate provider.

## V. System Maintenance Considerations

The credit union's information systems will likely require periodic maintenance. When new hardware, software, and operating system updates are made, they can impact the security of the system. Additionally, some maintenance may be needed to enhance the security of the system due to the discovery of security "holes" in the system. Proper change controls and timely patching of security vulnerabilities are critical to the security of member information systems.

## System Modifications

To avoid compromising system security, modifications must be in accordance with the credit union's system modification and configuration policy (e.g., audit features enabled, default system passwords changed, latest patches/updates installed, required testing completed, etc.).

## Patch Management

It is important that credit unions monitor necessary security patches as new vulnerabilities to existing systems are discovered very frequently. These vulnerabilities are often exploited by hackers in order to compromise computer systems.

Many system components are subject to inherent security vulnerabilities. These vulnerabilities are discovered on a frequent basis by hackers, security organizations, researchers, vendors, users, etc. Vulnerabilities can, if exploited, allow third parties to gain remote access and/or control over critical systems of the credit union. Significant vulnerabilities (or "holes") should be "patched" to avoid compromising system security.

To minimize the threat posed by security vulnerabilities, a "patch management" process should be in place.

- Review service provider and manufacturer websites to keep appraised of recommended system updates. Subscribe to e-mail notifications, if offered.

- Subscribe to on-line security bulletins. Numerous private and public sources of alerts are available that provide e-mail notification of new hacker exploits, viruses, and security-related software bugs. These bulletins will typically provide a recommended course of action to "patch" the hole. If a software update is necessary, the bulletin will often direct the reader to the site where the update can be downloaded.

- Determine the threat of the vulnerability to the credit union's information system environment. This analysis will dictate what, if any, action to take.

- Determine what impact the update may have on the system. Testing may be prudent to avoid any unforeseen consequences of installing an update to the production system.

- Evaluate the source of the security alert and recommended patch. Some "patches" have been known to introduce new vulnerabilities to systems.

- Run network-scanning software to identify weaknesses to known security vulnerabilities. There are commercial and freeware products available to assist with this process. Credit unions will need the appropriate technical expertise in order to understand and respond to the results.

**Maintenance Periods**

Security measures should not be lowered during maintenance periods if external access to credit union systems is still available. Hackers may take advantage of these brief periods to gain access to credit union systems.

## VI. System Monitoring and Incident Response Considerations

Procedures to detect and respond to actual and attempted attacks on or intrusions into member information systems can reduce the impact of these events. Key considerations include:

**Monitoring**

A process should be in place to ensure timely manual review of logs, reports, and alerts generated by system components (e.g., firewall, intrusion detection system, virus protection systems, etc.). Some systems can be programmed to provide real-time automated alerts and take limited predefined responses.

**Incident Response**

Develop a formal incident response plan to limit the damage from an attack. The plan should include the following key components:

- Incident response team comprised of appropriate areas of the credit union (e.g., legal, IT, security officer, audit, public relations, etc.) and possibly outside experts (e.g., legal, security experts, etc.).

- Specific responsibility and authority of staff and officials for reacting to incidents.

- Specific actions (including time frames), based on foreseeable scenarios (e.g., hacking, denial of service attack, etc.), including:

    a. Escalation procedures (e.g., monitoring the situation, disconnecting Internet connections, shutting down systems, protection of evidence, documentation of actions and time and other resources – which can be important for prosecuting cases and for possible bond claims, etc.); and

    b. Internal and external notifications (e.g., staff, officials, legal counsel, law enforcement, bond company, forensic experts, members, regulators, media, etc.).

Note, some third parties can remotely monitor and manage intrusion detection systems, virus protection, firewalls, routers, and thus play a role in the incident response plan.

## VII. Security Program Validation Considerations

Periodic testing of key controls, systems and procedures of the security program should be completed to validate their effectiveness. Methods can include:

- Self-audits by operational staff for compliance with the security program; and/or
- Independent assessments by the supervisory or audit committee, internal auditor staff, auditors or consultants. Related information appears in Chapter 10.

## VIII. Outsourcing Considerations

Outsourcing of e-Commerce activities does not alleviate the credit union from its responsibility to provide adequate security over member information. Therefore, the credit union should determine what control considerations (above examples) are applicable based on its unique e-Commerce environment. Then the credit union must ensure that adequate control measures are in place at the service provider(s), who acts on behalf of the credit union, to provide e-Commerce to the members. Note, even certain critical security services can be outsourced (e.g., remotely managing routers, firewalls, intrusion detection systems). Related information appears in Chapter 11.

# APPENDIX D – GLOSSARY

| Term | Definition |
|---|---|
| **Application** | A computer program or set of programs that perform the processing of records for a specific function. |
| **Application Service Provider (ASP)** | An organization that hosts software applications on its own servers within its own facilities. Customers access the application via private lines or the Internet. |
| **Assessment** | A review, the scope of which should be expressly stated, to determine the adequacy of current controls for a given area (network security, website compliance, etc.). |
| **Audit Policy** | Defines the type of security events that are logged for a domain or for individual computers; determines what the operating system will do when the security log becomes full. Audit policy can track the success or failure of specified security events. |
| **"Auditability"** | The degree to which transactions can be traced and audited through a system. |
| **Authentication** | 1) The process that assures the receiver of a digital message of the identity of the sender. It also is used to validate the integrity of the message.<br>2) The process of proving the claimed identity of an individual user, machine, software component or any other entity. |
| **Authorization** | Process to verify the identity and legitimacy of a user logging on to a computer system. |
| **Batch Processing** | The processes of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity. |
| **Biometrics** | Processing a group of transactions at one time. Transactions are collected and processed against the master files (master files updated) at the end of the day or some other time period. |
| **Browser** | Method of verifying identity by analyzing a unique physical attribute. |
| **Cable** | A computer program that enables the user to retrieve information that has been made publicly available on the Internet; also permits multimedia (graphics) applications on the World Wide Web. |
| **Cache** | A type of Internet access that is faster than dial-up connections and works over the cable TV (CATV) infrastructure. |
| **Code** | Cache is high-speed memory that is used to speed up data transfer and may be either temporary or permanent. Browser/Internet caches keeps copies of the most-recently requested web pages in memory or on disk in order to speed up retrieval. Pages will be deleted from the cache after a set amount of non-activity. |
| **Connectivity** | Computer programs. |
| **Dedicated** | Refers to communications networks or the act of communicating between computers via devices such that link networks together. |
| **Demilitarized Zone (DMZ)** | Assigned to only one function. |
| **Denial of Service Attack** | A barrier between the Internet and a company's internal network utilizing a firewall. Dual firewall architecture may add an extra measure of security for the internal corporate network. |
| **Design Phase** | An attempt to overwhelm a server with requests so that it cannot respond to legitimate traffic. |
| **Dial-up** | The phase during which the problem solution that was selected in the Study Phase is designed. The design includes the allocation of system functions; the design of inputs, outputs, and files; and the identification of system and component requirements. |
| **Digital Subscriber Line (DSL)** | The ability of a remote user to access a system by using private or common carrier telephone lines. |
| | A type of Internet connection that utilizes existing copper phone lines, but is faster than a typical dial-up connection. DSL allows subscribers to use their telephone while simultaneously keeping a constant Internet connection. |

| Term | Definition |
|---|---|
| **Domain Name** | A unique alphanumeric name for an organization's website. |
| **E-mail** | Messages people send to one another electronically from one computer to another. |
| **Encryption** | The process of scrambling data by a device or encoding principle (mathematical algorithms) so that the data cannot be read without the proper codes for unscrambling the data. Also, see VPN. |
| **Feasibility Analysis** | The process of determining the likelihood that a proposal will fulfill specified objectives. |
| **File Transfer Protocol (FTP)** | A standard way of transferring files from one computer to another on the Internet. "Secure" FTP strategies add a layer of protection to the files being transferred to reduce the likelihood of the files and data being inappropriately accessed by unauthorized persons while in transit over the Internet. |
| **Firewall** | A system or combination of hardware and software solutions that enforces a boundary between two or more networks (or sub-networks). |
| **Freeware** | Software available without charge. |
| **Hacker** | A computer operator who breaks into a computer without authorization, for malicious reasons, just to prove it can be done, financial gain, or other personal reasons. |
| **Hardware** | Machinery and equipment (central processing unit, disks, tapes, modem, cables, PCs, etc.). |
| **Host** | A computer that provides services directly to other computers. |
| **Identity Theft** | The act of stealing another person's identity. Identity theft occurs when someone appropriates personal information (e.g., name, social security number, account number, etc.) without permission in order to commit fraud or theft. |
| **Incident Response Team** | A team of computer experts (internal or external) organized to protect an organization's data, systems, and other assets from attack by hackers, viruses, or other compromise. |
| **Infrastructure** | The basic, fundamental architecture (e.g., hardware, software, controls, etc.) of any system. This determines how the system functions and how flexible it is to meet future requirements. |
| **In-house** | Computer operations that take place on the credit union's premises with the credit union directing the day-to-day operation of the computer systems. |
| **Internet** | A worldwide network of computer networks. |
| **Internet Banking** | Services that allow a member to interact with a credit union from a remote location by using a telephone, television set, terminal, personal computer, or other device to access a telecommunication system which links to the institution's computer system. |
| **Internet Service Provider (ISP)** | An entity that provides access and/or services related to the Internet, generally for a fee. |
| **Interoperability** | The compatibility of distinct applications, networks, or systems. |
| **Intrusion Detection System (IDS)** | Software that performs real-time automated reviews of security logs (and/or network traffic) data to detect and alert to potential unauthorized user activity. |
| **Login (logon)** | Process of identifying oneself to the network and gaining access to network resources. |
| **Magnetic Stripe** | Used on identification cards to store encoded information read by card readers. |
| **Network** | A group of computers connected by cables or other means and using software that enables them to share equipment and exchange information. A system of software and hardware connected in a manner to support data transmission. |
| **Non-repudiation** | The electronic transaction documentation must be in a form the member cannot deny, disown, recant, disavow, disclaim, or retract. The origin or the receipt of a specific message must be verifiable by the credit union and/or a third party. |
| **On-line** | Equipment or devices that communicate with a computer network. Connections can be direct (as in a network using dedicated connections) or indirect (as in using the Internet). |
| **Outsourcing** | Contracting with outside consultants, software organizations or service bureaus to perform systems analysis, programming and data center operations. |
| **Password** | A unique word or string of characters that a programmer, computer operator, or user must supply to satisfy security requirements before gaining access to the system or data. |
| **Penetration Testing** | Using automated tools to determine a network's vulnerability to unauthorized access. |

| Term | Definition |
|---|---|
| **Personal Computer (PC)** | A computer that serves one user in the office or at home. With the addition of a modem or network card, the personal computer becomes a terminal capable of retrieving information from other computers, online services and the Internet. |
| **Real-time** | System provides an immediate response (e.g., logging, monitoring, or processing) rather than storing the data for later action. |
| **Remote Access** | Letting off-site users access a central network. |
| **Repudiation** | The denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication. |
| **Router** | A computer system in a network that stores and forwards data packets between local area networks and wide area networks. |
| **SAS 70 Report** | Statement of Auditing Standards (SAS) 70 review - "Reports on the Processing of Transactions by Service Organizations." This report is the result of an independent review and is intended for the financial auditors of the service provider's clients. Type I report describes controls at the service provider at a point in time. Type II report is based on testing of controls over a given period of time. Reports may contain user considerations for controls that may be needed at the credit union. The SAS 70 report does not provide an opinion on e-Commerce security or disaster recovery. |
| **Scalable** | The ability of a system to support high-growth enterprise applications. These applications are typically large-scale, mission-critical in nature. Examples include supporting widely used online banking activities, hosting popular websites, maintaining large data warehouses, and administering large e-mail systems. |
| **Scan** | Software that is run to detect and report security vulnerabilities on computers, websites, networks, firewalls, routers, etc. |
| **Server** | A computer dedicated to servicing requests for resources from other computers on a network. |
| **Service Bureau** | Outside information processing services that take place in an environment that is physically separate from the credit union's operations and for which credit union management is not in direct control. |
| **Service Provider** | A vendor that provides technology services to credit unions such as a telephone company, core share and loan provider, an Internet service provider (ISP), an application service provider (ASP), etc. |
| **Social Engineering** | Posing as a manager, technician, service provider personnel, IS staff, or other likely authorized person, in order to fool unsuspecting employees in to providing user ids, passwords, physical access, or downloading files (with malicious code). Information is used by hackers to gain access to the system |
| **Software** | Instructions for the computer. A series of instructions that perform a particular task is called a "program." The two major categories of software are "system software" and "application software." System software is made up of control programs such as the operating system and database management system. Application software is any program that processes data for the user (payroll, spreadsheet, word processor, core share and loan program, etc.). A common misconception is that software is data. It is not. Software tells the hardware how to process the data. Software is "run." Data is "processed." |
| **System Policy** | A policy used to control what a user can do and the environment of that user. System policies can be in Windows NT, applied to a specific user, group, computer, or all users. System policies work by overwriting current settings in the registry with the system policy settings. |
| **Trojan Horse** | A program that appears to perform a useful function and sometimes does so quite well but also includes an unadvertised feature, which is usually malicious in nature (e.g., creating a backdoor through which hackers can enter the system). |
| **Upload** | To transmit a file to a central computer from another computer or a remote location. |
| **Virus** | A program with the ability to reproduce by modifying other programs to include a copy of itself. It may contain destructive code that can move into multiple programs, data files, or devices on a system and spread through multiple systems in a network. |

| Term | Definition |
|---|---|
| **Virtual Private Network (VPN)** | A private network that is configured over public telecommunication lines. VPNs enjoy the security of a private network via access control and encryption to protect against hackers, while taking advantage of the economies of scale and built-in management facilities of large public networks. |
| **Vulnerability** | A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security. |
| **Web (a.k.a. World Wide Web)** | A sub-network of the Internet through which information is exchanged via text, graphics, audio, and video. |
| **Web Page** | Information presented through a web browser in a single view ("page"). |
| **Web Server** | A computer that provides web services on the Internet. It includes the hardware, operating system, web server software, and the website content (web pages). |
| **Website** | A web page or set of web pages designed, presented, and linked together to form a logical information resource and/or transaction initiation function. |
| **Wireless** | Radio transmission via the airwaves. Various communications techniques are used to provide wireless transmissions. |
| **Worm** | A program that scans a system or an entire network for available, unused space in which to run. Worms tend to tie up all computing resources in a system or on a network and effectively shut it down. |