# CORPORATE CREDIT UNION GUIDANCE LETTER

No. 2004-03 DATE: August 9, 2004

SUBJ: Critical Information System Risk Areas

TO: The Corporate Credit Union Addressed

Information technology (IT) and security continue to evolve at a rapid pace. New risks and threats arise quickly to challenge emerging and established technologies. Yet the essential elements of strong controls and sound IT practices remain the same despite the environmental changes.

As part of our review of IT in corporate credit unions, the Office of Corporate Credit Unions (OCCU) IT examiners have focused on ensuring the adequacy of basic control elements such as firewalls, intrusion detection, penetration tests, and sound network architectures. I am pleased to note that corporates have been diligent in this regard and that many sound control practices have been implemented.

OCCU IT staff will continue to verify that basic IT security control elements remain strong. However, the ever changing dynamics of the corporate credit union IT risk profile require that we also focus attention on the following critical information security areas:

1. Information Security Risk Assessment;
2. Security Application Code Reviews;
3. Service Provider Oversight & Contracts;
4. Security Awareness of Employees;
5. Change Management for Applications & Infrastructure; and
6. Security for Remote Locations.

Each area is briefly discussed below. Additional information, supporting references, and footnotes follow at the end of this letter.

**Information Security Risk Assessments** - Information security best practices prescribe the implementation of an institutional risk assessment as a necessary pre-requisite to the formulation of an information security strategy. The risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. An adequate assessment identifies the value and sensitivity of information and system components and then

balances that knowledge with the exposure from threats and vulnerabilities. Benefits resulting from this process include:

1. Proactive management of information security risks - identifying risks before they impact the institution;

2. Enhanced knowledge - providing for a complete system characterization and identification of critical data and risk exposures; and

3. Accountability - information owners assume ownership for the risk exposures. The risk assessment is the key driver for the rest of the information security process.[1]

Risk assessments for most industries focus only on the risk to the business entity. However, section 501 (b) of the Graham Leach Bliley Act (GLBA) requires financial institutions to "protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer." Therefore, financial institutions must also consider the risk to their customers' information. Accordingly, Appendix A of Part 748 of NCUA's Rules and Regulations, calls for credit unions to "identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems, and assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information." This statement describes the essence of a risk assessment.

An initial risk assessment involves a significant one-time effort but once completed should only require minimal efforts to maintain and update. FFIEC guidelines enumerate several key practices for the effectiveness of a risk assessment as follows:

1. Multidisciplinary - Involving a broad range of users with a range of expertise and business knowledge;

2. Systematic and centrally controlled - Central control and coordination will facilitate an organizational view of risks and lessons learned from the risk assessment process;

3. Integrated - Providing a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of testing those controls;

4. Accountable - Involving the board and upper management;

5. Documented - The documentation of risks accepted and risk mitigation decisions is fundamental to achieving accountability for risk decisions;

6. Providing Enhanced Knowledge - Risk assessment increases management's knowledge of the institution's mechanisms for storing, processing, and communicating information, as well as the importance of those mechanisms to the achievement of the institution's objectives; and

7. Regularly Updated - Updated as new information affecting information security risks are identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change or configuration change) with senior management reviewing the entire risk assessment at least annually.

**Security Application Code Reviews -** Critical Internet-facing web applications should undergo a security code review by qualified staff, independent of those responsible for the application development, or an independent third party to identify unknown security vulnerabilities. This applies to both internally and externally developed or purchased web applications, as well as those hosted by the corporate or residing with a third-party provider. Protecting GLBA member information that passes through these applications is critical. Security code reviews are complementary to, but provide a different internal perspective than, external network-based vulnerability penetration tests. Code reviews can be completed manually. However, new intelligent-based automated software tools and utilities are emerging that can perform the work more efficiently and at less cost. Code reviews for Intranet-based web applications are encouraged. Application security code reviews should be performed prior to initial application deployment and again subsequently whenever the application undergoes significant change. [2]

**Service Provider Oversight Process & Contracts -** Organizations remain responsible for their processes whether they choose to perform services themselves, or seek the assistance of third-parties in providing them. This is also true for protecting GLBA member data. Corporate credit unions that outsource work to third parties should have:

1. An internal service provider oversight process in place that ensures that adequate provider protections and controls are functioning and that appropriate expectations are communicated and met; and

2. A written contract in place with the provider that can legally enforce those elements, as required. [3]

Corporates should consider the following security-related issues when selecting or monitoring a service provider:

1. Service provider references and experience;

2. Security expertise of contracted personnel;

3. Background checks on contracted personnel;

4. Contract assurances regarding security responsibilities and controls;

5. Nondisclosure agreements covering the institution's systems and data;

6. Ability to conduct audit coverage of security controls or provisions for reports of security testing from independent third parties; and

7. Clear understanding of the provider's security incidence response policy and assurance that the provider will communicate security incidents promptly to the institution when its systems or data are potentially compromised.

**Security Awareness of Employees -** Organizations dedicate significant resources to deploy appropriate network security architectures, processes and controls. However, even the most elaborate protection mechanisms can be bypassed by individuals seeking to exploit system weaknesses. Exploit attempts may come from both internal sources (employees) and external sources (hackers). The most important element in recognizing these attempts is vigilant employees with a strong sense of security awareness who immediately report suspicious activity to their organization's security officer. The process starts with employee training and their written acknowledgement that they understand the organization's computer and Internet use policies as well as account/password policies. On-going security awareness is achieved through a program or campaign that employs multiple communication channels and is sustained throughout the year. Periodic internal testing or verification of individual employee security awareness is highly encouraged. [4]

**Change Management for Applications & Infrastructure -** Change management processes outline controlled procedures for making both planned and emergency changes to:

1. Software applications;

2. Application data;

3. Databases;

4. Operating systems; and

5. All hardware infrastructure elements.

These documented procedures require process owner approval for each change, and maintaining a historical record of changes made that include the date and time of the change, brief description of the change, who approved the change and who made the change. Where possible, security controls enforce adherence to the change management process through preventative, front-end controls and/or back-end detective controls with appropriate audit logs and review processes. [5]

**Security for Remote Locations -** Many organizations have strong network security architecture and complimentary, well-controlled security administration processes for their central office location. Some organizations also have remote locations (e.g., CUSOs, IPS sites, sales offices, etc.). Appropriately sized security elements that comprise a strong program at the central office should also be employed to address remote sites. Examples include security administration and periodic account reviews, security awareness programs, sound security architectures, protection mechanisms for servers and clients, and security monitoring. [6]

OCCU remains committed to working with each corporate credit union in exploring and developing the most appropriate means for addressing its unique critical information security risk areas. We welcome your comments both during and outside the context of the examination process. We will continue to share "best practices" with all corporates on an ongoing basis.

Sincerely,

/S/

Kent D. Buckham
Director
Office of Corporate Credit Unions

cc: NASCUS
NAFCU
ACCU
State Regulators

**References and Footnotes:**

[1] **Security Risk Assessment** — See NCUA Part 748, Appendix A, Parts II and III for a description of, and requirements for, a formal, written, sustained security risk assessment process. Also see FFIEC Information Security Handbook, December 2002, pp. 7-14, A-3. The following Risk assessment methodologies/models may also be helpful.

- National Institute of Standards, NIST SP 800-30 Rev A, Risk Management Guide for Information Technology Systems. See http://csrc.nist.gov/publications/nistpubs/index.html
- Operationally Critical Threat, Asset, and Vulnerability Evaluation, OCTAVE & OCTAVE-S, by Christopher J. Alberts, Audrey J. Dorofee, CERT, Software Engineering Institute (SEI), Carnegie Mellon University. See http://www.cert.org/octave/
- STAR Methodology by Randy Marchany, Information Services, Virginia Tech University. See http://security.vt.edu/playitsafe/index.phtml#RiskAnalysis

[2] **Application Security Code Reviews** — See FFIEC Information Security Handbook, December 2002, pp. 57, A-6, A-17. The following resources may also be helpful:

- National Institute of Standards, NIST SP 800-30 Rev A, Risk Management Guide for Information Technology Systems, Security test and evaluation (ST&E), pg16, paragraph 3.2.2 System Security Testing. http://csrc.nist.gov/publications/nistpubs/index.html
- *Secure Coding: Principles and Practices*, by Mark G Graff & Kenneth R. Van Wyk, O'Reilly & Associates, © 2003, ISBN: 0596002424
- *How to Break Software Security*, by James A. Whittaker, Herbert H. Thompson & Herbert Thompson, Pearson Education, 2003, ISBN: 0321194330

[3] **Service Provider Oversight** — See NCUA Part 748, Appendix A, Appendix A, Part III(d) and FFIEC Information Security Handbook, December 2002, pp. 66-67, 81, A-5.

[4] **Security Awareness** — See FFIEC Information Security Handbook, December 2002, pp. 55-56, 60-62, 82, A-6. The following publications and web sites may also be useful: NIST-SP800-50 Building Security Awareness, see http://csrc.nist.gov/publications/nistpubs/index.html; http://www.humanfirewall.org/resources.htm; http://searchsecurity.techtarget.com/home/

[5] **Change Management** — See FFIEC Information Security Handbook, December 2002, pp. 57, A-17, A-12, A-15 and FFIEC Development and Acquisition Handbook, April 2004, pp. 51-54, 64-65.

[6] **Security for Remote Locations** — See FFIEC Information Security Handbook, December 2002, pp. 15-66, 82-83.