Information Technology (IT)
Summary of Information Request

This information is the property of the Division of Credit Unions and is received from the credit union for our confidential use.

Under no circumstances may any recipient of this examination information use, disclose, or make it public except as authorized relating to credit union regulation. The law provides penalties for unauthorized use or disclosure of any such information, which is not otherwise publicly available. If any subpoena or other legal process is received calling for the production of such information, you should notify the DCU immediately.

General Directions

Reports and information should be the most recent available. If you cannot provide the documents requested, please indicate why. If a particular area is not applicable, simply indicate N/A.

Supporting Documentation

The IT examiners will be examining the Credit Union for a variety of IT controls. The numbered information requests below comprise the standard documentation required by the examiners. Additional documentation and information may be required during the course of the exam.

To the extent possible and appropriate please provide the following documentation on a CD, organized by section and item number and have it ready for the examiners when they arrive. Please contact Glenn Ross at 360-481-2551 if you will not be able to accommodate this request.

Section 1. General:

1. Provide all policies and procedures that relate to information technology management, E-commerce, electronic delivery systems, and information security.
2. Provide policy/agreement concerning acceptable usage of network (computer, internet, email, etc.) resources by employees/volunteers.
3. Provide reports that were presented to the board of directors from the Information Technology Committee or any other committees or individuals regarding information technology and security initiatives for the most recent 12 months.
4. Provide a written status for each issue and finding from the prior IT exam.

5. Provide a summary of the applications and systems used by completing the table below:

Category of System	Vendor, Application Name & Release Number	Operating System Name & Version Number	Outsourced or Hosted Internally?	If Outsourced, a current SAS70 report on file?
Core Processing				
Item Processing				
Imaging System				
Online Banking				
Telephone Banking				
Statement Printing				
Credit Card Processor				
Debit Card Processor				
Bill Pay				
Check Printing				
Other (specify):				

Section 2. Risk Assessment

2.1. Provide a copy of the Credit Union's Risk Assessment to fulfill NCUA 12 CFR 748 appendix A Item III. B.

Section 3. Audit and Testing Services

3.1 Provide most recent internal and/or external risk review reports (audit, vulnerability assessment, penetration testing, key controls testing fulfilling NCUA 12 CFR 748 Appendix A Item III. C. 3, etc.) along with management's response.

3.2 Provide a) copies of documentation describing all IT and/or member information security incidents, investigations and responses, and b) copies of any related Suspicious Activity Reports.

Section 4. Vendor Management

4.1 Provide a copy of the credit union's Vendor Management Policy and Process.

4.2 Provide a list of critical vendors and vendors with access to member data. Indicate

- the service provided
- how the vendor has access to, or stores member data.
- the date of the last SAS70 report along with the date it was reviewed by the credit union.
- the date that the contract with the vendor was last reviewed for vendor management policy compliance.

4.3 Provide a) the latest audit reports (e.g. SAS70 Type II) from vendors with access to member data, and b) documentation of your credit union's review of the vendor audit reports including an analysis of any SAS70 findings and client control considerations.

4.4 Provide access to vendor contracts/service agreements and documentation indicating contracts contain language

- requiring confidentiality/security of member information according to Gramm-Leach-Bliley Act requirements,
- requiring notifying the credit union if the vendor suspects loss of member information, and
- describing the return/destruction of member information upon contract termination.

Section 5. Personnel

5.1 Provide the organization chart for the IT department.

5.2 Provide job descriptions, profiles, professional certifications and training plans for IT personnel.

Section 6. System Architecture and Controls

6.1 Provide a Network Topology Diagram (do not include IP addresses) showing network devices such as firewalls, routers, servers, modems, and all connections to public networks or third parties.

6.2 Provide copies of any firewall rule configurations (include comments explaining the purpose of each rule and each open port).

6.3 Provide a list of all hardware and software inventory along with any reviews/audits indicating compliance with credit union software/hardware policies.

Section 7. Security Controls

7.1 Provide inventory of security hardware and software, including firewalls, intrusion

detection/prevention systems, encryption, user authentication components, virus protection, etc.

7.2 Provide copies of recent reports (30 days) relating to routine security monitoring, e.g., firewall logs, VPN logs, web access reviews, intrusion detection/prevention reports.

7.3 Provide access control logs showing additions, changes and deletions of employee accounts and privileges. Also provide documentation of periodic management review of employee core processing system usage privileges.

7.4 Provide a listing of users with access to the core processing system, access to the network, and remote access (e.g., VPN).

7.5 Provide network and core processing system user account security settings (passwords, lockout, timeout, screen saver, etc.)

7.6 Describe physical security controls for credit union computers and other IT equipment..

7.7 Provide evidence of updates to virus protection and intrusion detection applications.

7.8 Provide evidence that critical server and workstation patches have been applied. For any critical patches that have not been applied, please provide documentation to support the decision not to apply critical patches.

7.9 Describe policy, as well as the technical and administrative processes employed by the credit union for remote access to the internal network, workstations, devices, etc. by employees and/or third parties.

7.10 Describe mobile device (laptops, PDA, flash drive, external drive, etc.) security policies and implementation.

7.11 Describe wireless (802.11abg, Bluetooth, Blackberry/PDA, etc.) usage policies and processes.

Section 8. Business Continuity

8.1 Provide the Disaster Recovery/Business Continuity Plan for the recovery of IT systems and operations.

8.2 Provide reports relating to the tests of any Disaster Recovery/Business Continuity plans that were done within the last 18 months.

8.3 Describe the process for creating, transporting, storing and retrieving backup tapes.

8.4 Provide a list of backup tapes, disks, documentation, supplies, etc. kept at on and off-site storage facilities.

8.5 Provide Disaster Recovery agreements with Service Providers.