	A	B	C	D
3		**IT - Items Needed**		
4		**Comment to the Credit Union: This is a listing of items needed for your upcoming IT review. All items should be available at the start of the examination. Please number the items to correspond with the numbering system below. Wherever practical, please provide electronic versions of documents or reports. If an item is unavailable during the review, please state why in the comment box.**		
5			**R**	**Comments**
6		**Section A: Strategic Risk**		
7	1	Provide IT related policies such as:		
8	1a	(a) Physical and Data Security		
9	1b	(b) E-Commerce		
10	1c	(c) Computer Use Policy including Internet and E-mail use (provide an example of acknowledgement forms signed by employees)		
11	1d	(d) Networking (including Communications, Routers, Servers, Workstations, Remote Access, etc.)		
12	1e	(e) Firewall		
13	1f	(f) System Acquisition and Change Management		
14	1g	(g) Vendor Oversight		
15	1h	(h) Software Development and Maintenance (If Applicable)		
16	1i	(i) Capacity Planning		
17	1j	(j) Auditing and Monitoring		
18	1k	(k) Backup and Recovery/Records Preservation Program		
19	1l	(l) Business Continuity/Disaster Recovery		
20	1m	(m) Incident or "Outage" Response		
21	2	Minutes of IT committee meetings.		
22	3	Recent monthly performance monitoring reports.		
23	4	Long-term strategic plans, if any, that relate to IT goals and strategies.		
24	5	Internal audit plans, if any, to review IT as well as results of any IT reviews done since the last examination.		
25	6	Most recent risk review reports/comments on IT or e-commerce along with management's response.		
26	7	Summary of insurance policy coverages for e-commerce, electronic crime, and loss of records/equipment.		
27	8	Listing of IT vendors and service providers.		
28	9	Key vendor contracts and evidence of contract reviews.		
29	10	Results of recent disaster recovery tests, including the scope of test procedures performed.		
30	11	Summary of planned changes, if any, to key personnel, software, hardware, or operating procedures.		
31	12	Board reports on IT security, program changes, results of vulnerability assessments, intrusions, etc.		
32	13	Minutes of Supervisory Committee meetings.		
33		**Section B: Transaction Risk**		
34	14	Listing of IT administrators and security officers. Provide a description of experience, training, and certifications related to IT.		
35	15	Listing of personnel and vendors with special access privileges to administer operating systems, networks, and applications.		
36	16	Last audit review of employee access privileges and controls for timely removals or modifications.		

	A	B	C	D
3		**IT - Items Needed**		
4		**Comment to the Credit Union: This is a listing of items needed for your upcoming IT review. All items should be available at the start of the examination. Please number the items to correspond with the numbering system below. Wherever practical, please provide electronic versions of documents or reports. If an item is unavailable during the review, please state why in the comment box.**		
5			**R**	**Comments**
37	17	Recent Security Override and Administrator Log Reports.		
38	18	Procedures for reviewing override and administrator logs.		
39	19	List of employees, vendors, and officials with remote access privileges.		
40	20	Logging and review procedures for firewalls and intrusion detection/intrusion prevention systems.		
41	21	Listing of key software and electronic services (include audit/monitoring software).		
42	22	Inventory list of IT equipment (include servers and a list of services offered on each).		
43	23	Network topology diagram (databases, servers, routers, firewalls, communication lines, and remote access).		
44	24	Results of recent security assessments and vulnerability scans (include management's response).		
45	25	External audits done on IT control procedures.		
46	26	Due diligence reviews of vendors (include contract reviews, analysis of financials, review of SAS 70s, vulnerability scan summaries, business continuity tests, Trusecure certifications, etc.).		
47	27	List of firewall rules (include comments explaining the purpose of each rule and each open port).		
48		**Section C: Compliance Risk**		
49	28	Self assessment or internal audit reviews of compliance for IT products and services (include website).		
50	29	Records Preservation policy and Records Storage Log.		
51	30	Information Security Program in compliance with Part 748, Appendix A.		
52		**Section D: Reputation Risk**		
53	***31***	***Summary of relationships with CUSOs providing electronic services.***		
54	32	List of weblinking relationships (include agreements and due diligence reviews of linked partners).		
55	33	Review procedures for ensuring vendor compliance with Service Level Agreements.		
56	34	List of any IT incidents, intrusions, or attacks since the last examination (include management's response).		
57	35	Problem resolution procedures for member, employee, or vendor problems.		
58		**Overall Questionnaire Comments:**		

	A	B	C	D
3	**IT - Items Needed**			
4	**Comment to the Credit Union:** **This is a listing of items needed for your upcoming IT review. All items should be available at the start of the examination. Please number the items to correspond with the numbering system below. Wherever practical, please provide electronic versions of documents or reports. If an item is unavailable during the review, please state why in the comment box.**			
5			**R**	**Comments**
59				

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - General**		
6		**Objective: Evaluate policies, procedures, practices, and controls over the IT environment.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8		**Section A: Policies And Procedures**		
9	1	Does the credit union have written policies for each service and appliance in place?		
10	2	Do the policies contain step-by-step procedures which describe the process/guidelines used by employees who are responsible for implementing the service or operating the appliance?		
11	3	Do the policies assign responsibility to specific staff?		
12	4	Does the CU's bond include electronic crime coverage?		
13		Section Rating:		
14		**Section B: Physical Controls**		
15	5	Is the physical access to computer facilities adequately controlled?		
16	6	Is access to the computer facility limited to only appropriate employees in commensurate to the size and complexity of the credit union?		
17	7	Are the communication routers and patch panels that are not located within the computer facility adequately secured?		
18	8	Is there fire protection for the computer equipment/ facilities?		
19	9	Is there a UPS system utilized? Describe its capacity.		
20	10	Is the computer room climate adequately controlled?		
21		Section Rating:		
22		**Section C: User Controls**		
23	11	Does each employee have a unique password to access each system in use?		
24	12	Is there a Password Policy which address length and type of characters, frequency of password change, reuse of previous passwords, etc?		
25	13	Are passwords always set with an expiration date?		
26	14	Does the computer system lock out an employee after a number of failed log-on attempts?		
27	15	Do terminals lockout/timeout after not in use for a specified period of time?		
28		Section Rating:		
29		**Section D: Multiple System/Network Controls**		
30	16	Is there a system administrator responsible for changes in the network?		
31	17	Has the system administrator changed the default password for each software product?		
32	18	Is the system administrator's password unique from other access passwords?		
33	19	Are there various access levels assigned to employees?		
34	20	Is employee access changed when a user's duties change and removed promptly upon leaving employment?		

	A	B	D	F
5		**IT - General**		
6		**Objective: Evaluate policies, procedures, practices, and controls over the IT environment.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
35	21	Does anyone (system users or vendors) have access to the system from a remote location?		
36		Section Rating:		
37		**Section E: Internet Access**		
38	22	Does the credit union have access to the Internet? If no, skip this section.		
39	23	Has an Internet User Policy been approved by the board of directors?		
40	24	Do employees who have Internet access receive a copy of the Internet User Policy?		
41	25	Are employees who have Internet access required to signify receipt of the Internet User Policy by signing a document which is retained in the employees personnel file?		
42	26	Is Internet access limited to employees whose job responsibilities require access?		
43	27	What type of Internet access does the credit union have?		
44	27a	(a) Dial-up		
45	27b	(b) High Speed (DSL, cable, T-1,etc.)		
46	27c	(c) Wireless		
47	28	Is there software or other means which tracks employee Internet traffic/usage?		
48	29	For dial-up, are there adequate controls over modems?		
49	30	For those with Internet exposure, are there adequate security measure in place to control access to the network?		
50	31	Is virus protection software on all computers and is it updated on a regular basis?		
51		Section Rating:		
52		**Section F: E-Mail**		
53	32	Do credit union employees receive/send e-mail?		
54	33	Has an E-Mail Policy/Procedure Manual been approved by the board of directors?		
55	34	Does the employees E-Mail Policy or Acceptable Use Policy address appropriate/inappropriate messages for employees to comply with?		
56	35	Do employees receive a copy of the E-Mail/Acceptable Use Policy and are they required to signify acceptance by signing a document which is maintained in their personnel file?		
57	36	Is the e-mail server maintained by the credit union? If yes:		
58	36a	(a) Is the server maintained in a DMZ or another area outside of the computing network?		
59	36b	(b) Is only one service (e-mail) running on the server?		
60	36c	(c) Is virus software running on the server and is all e-mail scanned before allowing entry into the network?		
61	36d	(d) Is the virus software on the server updated on a regular basis?		

	A	B	D	F
5		**IT - General**		
6		**Objective: Evaluate policies, procedures, practices, and controls over the IT environment.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
62	36e	(e) Is there a policy on the types of attachments permitted to be attached to e-mails?		
63	36f	(f) Does the server have the ability to restrict the types of files which can be sent by employees?		
64	37	If the e-mail server is maintained by a third party, does the third party scan messages for viruses?		
65		Section Rating:		
66		**Section G: Website Review**		
67	38	Does the credit union have a website? If no, skip this section.		
68	39	Are there adequate policies/procedures for the website?		
69	40	Is the domain name registered in the name of the credit union?		
70	41	Is there an approval process for changes made to the website?		
71	42	Does the credit union have monitoring policies and procedures addressing weblinking relationships?		
72	43	If there are links, are members notified they are leaving the credit union's website?		
73	44	If the credit union corresponds or transacts business with members via the website, is that information adequately secured?		
74	45	Has the website received a compliance review?		
75		Section Rating:		
76		**Section H: Vendor Oversight**		
77	46	Did management evaluate the service provider reputation and performance (e.g. contact references and user groups and document the contact)?		
78	47	Did the credit union request and evaluate service providers financial condition initially and then annually thereafter?		
79	48	Did the credit union obtain and review audit reports (e.g., SAS 70 reviews, security reviews, risk assessments, etc.) as well as regulatory examination reports initially and annually thereafter?		
80	49	Did the credit union obtain adequate information about service provider security measures in place to protect the facility, member data, etc.?		
81	50	Did the credit union determine if service providers have appropriate insurance coverage and document confirmation of the coverage?		
82	51	Did the credit union review service provider contingency plans, testing of the plan, and incorporate the plan into the credit union disaster recovery plan?		
83		Section Rating:		
84		**Overall Questionnaire Comments:**		

	A	B	D	F
5	**IT - General**			
6	**Objective: Evaluate policies, procedures, practices, and controls over the IT environment.**			
7		**Question**	**Yes/No/ NA/**	**Comments**
85				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B9
Comment: Operating policies should exist for services such as web site, Internet banking, bill pay, and for each appliance such as firewalls, intrusion detection systems, etc. An appliance is a device that is dedicated to a specific function in contrast to a general-purpose computer.

Cell: B11
Comment: Policies should clearly state which individual(s)), generally by title or position, is/are responsible for developing policy, procedures, monitoring compliance, implementing corrective action, and providing recommended revisions.

Cell: B12
Comment: Electronic crime coverage generally covers loss of funds resulting from unauthorized access (i.e., hackers) into the computer system, a member that makes fraudulent changes to the electronic data or computer programs, and virus destruction of electronic data or computer programs. Computer Crisis Management coverage generally covers expenses incurred as a result of malicious attacks, such as defaced web site, denial of service attacks, a breach of computer security leading to the theft of confidential information, and computer extortion.

Cell: D13
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B14
Comment: The Network Controls Questionnaire provides additional guidance.

Cell: B15
Comment: Access can be controlled by lock and key, keypad, biometrics, etc.

Cell: B16
Comment: An entry log could be used to document entry into the computer facility.

Cell: B17
Comment: A patch panel is a group of sockets used to connect incoming and outgoing lines in communications and electronic systems. Patch panels allow for manually wiring the connections with small cables (patch cords), not automatic switching. Wireless patch panels are also available that provide the cross connections by flipping a switch rather than plugging in wires.

Cell: B18
Comment: Fire protection may include one or more of the following: water-based sprinklers, gas-based, chemical based, or fire extinguisher. The protection may be manual or automatic (preferred). FM200 (Great Lakes Chemical) and HFC-227 (DuPont Corporation) are an alternative fire suppression system agents used as a replacement for the ozone depleting Halon 1301 used extensively before 1994.

Cell: B19
Comment: UPS stands for Uninterrupted Power Supply. Capacity is the amount of time available to orderly secure or shut down any system on the UPS. Capacity also describes/identifies which systems are on the UPS. It is not uncommon for only critical systems to be connected to the UPS.

Cell: B20
Comment: The room should be maintained at a cool and relatively constant temperature at all times to prevent hardware failure. The room should be adequately ventilated and dry. It is not unusual for a computer room to have its own HVAC (heating, ventilating, air conditioning) system.

Cell: D21
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B23
Comment: Each system (primary share/loan/GL, lending software, OFAC, etc.) should require a user name and password to access. Each user should have their own unique (not a generic or shared log in to be used by all users) login credentials. Many systems allow for single sign on which means each user logs into, or authenticates to, one system and the user then has access to all systems to which they are permitted to have access.

Cell: B24
Comment: Strong passwords are preferred over weak passwords; however, not all systems allow the use of strong passwords. Strong passwords should be at least 6 characters and require a combination of 3 of the following: upper case; lower case; numbers; special characters.

Cell: B25
Comment: It is a good practice to require password changes, generally at least every 90 days. Many systems can automatically require/prompt password changes.

Cell: B26
Comment: Industry best practice allows for 3 unsuccessful log in attempts before disabling the account. Some systems automatically reset after a pre-established period of time and others require the user to contact the system administrator to reset the account and password (preferred method).

Cell: B27
Comment: Industry best practice is automatic timeout between 5 and 15 minutes. Timeout thresholds should be based upon the risks associated with a particular system and the sensitivity of the data which can be accessed through that system.

Cell: D28
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B29
Comment: This section is for more complex systems with a server or main controller which controls the network. The Network Controls Questionnaire contains additional guidance for this section.

Cell: B31
Comment: Many systems, hardware (servers, routers, firewalls, etc.) and software, come with a default administrator user name and password. These credentials are publicly known and place systems and data at risk if not changed when the system is installed.

Cell: B33
Comment: Employees should only be assigned access to systems and levels in accordance with their assigned duties and responsibilities.

Cell: B34
Comment: System access should be based upon each employee's job duty/description. Upon position change, an employee's system access should be modified commensurate with the access required to perform those duties. Upon employee termination (voluntary or involuntary), the employee's user account should be deleted immediately to prevent unauthorized access.

Cell: B35
Comment: If yes, you may want to complete the Remote Access Questionnaire.

Cell: D36
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B39
Comment: An Internet User Policy (IUP) is a written agreement, signed by employees, which sets out the permissible workplace uses of the Internet. In addition to describing permissible uses, an IAUP should specifically set out prohibited uses, rules of online behavior, and access privileges. The IUP should clearly state the penalties for violations of the policy, including security violations and vandalism of the system. Anyone using the credit union's Internet connection should be required to sign an IAUP, and know that it will be kept on file as a legal, binding document.

Cell: B42
Comment: Limiting Internet access to those individuals with a demonstrated business need helps to: (a) prevent unauthorized Internet activity and usage; (b) improve security (by reducing the number of computers exposed to the Internet); and (c) reduce Internet resources (bandwidth) by reducing the number of computers connected to the Internet pipe.

Cell: B45
Comment: DSL (Digital Subscriber Line) is a technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office.
T-1 is a 1.544 Mbps point-to-point dedicated, digital circuit provided by the telephone companies. The monthly cost is typically based on distance. T1 lines are widely used for private networks as well as interconnections between an organization's PBX (Private Branch Exchange) or LAN (Local Area Network) and the telco (telephone company).

Cell: B46
Comment: If yes, you may want to complete the WLANs (Wireless LANs) Questionnaire.

Cell: B48
Comment: Adequate controls may include: (a) preventing unauthorized modems from being installed; (b) limiting online time by instituting a time-out function (if possible); (c) requiring disconnecting or powering off modems when not in use.

Cell: B49

Comment: High speed Internet access generally provides for constant Internet access and a firewall or other appliance would protect against unauthorized access to the network.

Cell: B50
Comment: Virus software can be located on a network server and/or each PC. Virus software (program and definition files) should be updated at a minimum weekly, preferably daily. Many virus programs can automatically obtain the updated files on a predetermined schedule and then "push" those updates out to the computers and servers on the network.

Cell: D51
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B52
Comment: NCUA Letters to Credit Unions Numbers 04-CU-12, 04-CU-06, 04-CU-05 contain additional information on this area.

Cell: B54
Comment: The policy should address at least: 1. Prohibited Use (The e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.); 2. Personal Use (Using a reasonable amount of resources for personal e-mails could be acceptable, but nonwork related e-mail shall be saved in a separate folder from work related e-mail. Sending chain letters or joke e-mails from an e-mail account should be prohibited.) 3. Monitoring (Employees shall have no expectation of privacy in anything they store, send, or receive on the e-mail system. Messages may be monitored without prior notice.) 4. Data Type (Employees shall not e-mail sensitive or confidential data or information unless approved by a supervisor and the data or information is properly encrypted.) 5. Enforcement (Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.); 6. Administration (Who is responsible for monitoring the e-mail system, the reports they generate, how often they are generated, and to who they are distributed); and 7. Retention (How long various types of e-mail must be maintained and the acceptable media for retention).

Cell: B58
Comment: DMZ (Demilitarized Zone) - A part of a network that is protected by a firewall, but may be accessed by external Internet clients. The DMZ generally contains servers such as SMTP servers, remote access machines, or web servers. Client machines and internal servers that do not need to be accessed by Internet clients are kept in a more protected segment of the network than the DMZ.

Cell: B59
Comment: Ideally, only one service should run on each server which faces the Internet. If a credit union runs multiple services on one server (i.e. email services, web services, etc.) and one of those services is compromised by a hacker, then all services and data on that server is highly vulnerable.

Cell: B60
Comment: An effective means of preventing viruses, Trojan horses, and/or other malicious malware is to prevent e-mails with such malware from reaching the end user. This e-mail screening is typically done at the server level.

Cell: B61
Comment: Virus software (program and definition files) should be updated as a minimum weekly, preferably daily. Many virus programs can automatically obtain the updated files on a predetermined schedule and then "push" those updates out to the computers and servers on the network.

Cell: B62
Comment: Files such as exe, ActiveX, etc. present higher risk to the network.

Cell: B63
Comment: One of the most common ways for a computer virus to be transmitted is by e-mail file attachment. One way to address this problem is to filter the types of files which employees may receive and/or send. Attachments can be filtered by their actual name or by type (.exe, .msi, .vb, .vbs. etc.). Limiting the types of attachments employees may e-mail also helps protect credit union or member confidential information.

Cell: D65
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B69
Comment: It is possible a credit union can own more than one domain name. NCUA Letter to Credit Unions 02-CU-16 provides additional guidance on domain name controls.

Cell: B70
Comment: Approved changes need to be documented, retained, and followed-up to verify changes.

Cell: B71
Comment: Weblinking relationships need to be monitored to ensure only those companies, organizations, and/or individuals who have been properly approved are listed on the web site.
See NCUA Letter 03-CU-08 on weblinking relationships.

Cell: B73
Comment: Any communication between the credit union and its members which contains sensitive or confidential information should be encrypted. Encryption is a communications process that scrambles private information to prevent unauthorized access as information is being transmitted between the member's browser and the credit union.

Cell: B74
Comment: Examples of compliance requirements: NCUA Logo, Home Equity Loan Disclosures, Equal Credit Opportunity Act, Equal Housing Lender Logo, COPPA, etc.

Cell: D75
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B76
Comment: For additional guidance, see NCUA Letters: 01-CU-20 Due Diligence Over Third Party Service Providers; 01-CU-04 Integrating Financial Services and Emerging Technology; and 00-CU-11 Risk Management of Outsourced Technology Services.

Cell: B77
Comment: Prior to entering into a contract for services, officials and management should evaluate the ability of the proposed vendor to meet the credit union's needs and expectations. See LTCUs 01-CU-20 Due Diligence Over Third Party Service Providers and 00-CU-11 Risk Management of Outsourced Technology Services for additional guidance.

Cell: B82
Comment: It is not unusual for a service provider to not disseminate detailed information concerning the results of contingency testing. However, in those instances the credit union should seek a summary of the results, a summary of the vendor's plan to resolve any issues, and a timeframe by which those issues are to be resolved.

Cell: D83
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - 748 Compliance**		
6		**Objective: Ensure management has considered the requirements and guidelines related to information technology initiatives.**		
7		**Question**	**Yes/No/ NA/**	**Comment**
8		**Section A: Part 748 - Security Program**		
9	1	Does the credit union have a written security program designed to:		
10	1a	a) Protect each credit union office from robberies, burglaries, larcenies, and embezzlement; (748.0(b)(1))		
11	1b	b) Ensure the security and confidentiality of member records;(748.0(b)(2))		
12	1c	c) Protect against anticipated threats or hazards to the security or integrity of such records;(748.0(b)(2))		
13	1d	d) Protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;(748.0(b)(2))		
14	1e	e) Assist in the identification of persons who commit or attempt such actions and crimes;(748.0(b)(3))		
15	1f	f) Prevent destruction of vital records as defined in R&R Part 749; (748.0(b)(4))		
16	2	Does the credit union have as part of its information security program, procedures to properly dispose of any consumer information the Federal Credit Union maintains or otherwise possesses, as required under Part 717.83 of the NCUA R&R? (748.0 (c))		
17		Section Rating:		
18		**Section B: Part 748 Appendix A - Safeguarding Member Information**		
19	3	Is the board of directors, or an appropriate board committee, involved in developing and implementing the Member Information Security Program ? (III. A)		
20	4	Does the credit union have a documented risk assessment process? (III. B)		
21	5	Is the credit union properly managing and controlling risk by mitigating risks identified in the risk assessment process, in line with the sensitivity of the information, likelihood of threat, and potential damage of identified threats? (III. C)		
22	6	Has the credit union adopted appropriate security measures to address the following? (III. C. 1)		
23	6a	(a) Access controls on member information systems? (III. C. 1.a)		
24	6b	(b) Physical access controls to facilities and equipment where data files and archives of sensitive member information are maintained. (III. C. 1.b)		
25	6c	(c) Encryption of electronic member information either in transit or storage where unauthorized individuals may gain access. (III. C. 1.c)		
26	6d	(d) Change control procedures designed to ensure that system modifications are consistent with the credit union's information security program. (III. C. 1.d)		

	A	B	D	F
5		**IT - 748 Compliance**		
6		**Objective: Ensure management has considered the requirements and guidelines related to information technology initiatives.**		
7		**Question**	**Yes/No/ NA/**	**Comment**
27	6e	(e) Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information. (III. C. 1.e)		
28	6f	(f) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems. (III. C. 1.f)		
29	6g	(g) Response programs that specify actions to be taken when the credit union suspects or detects unauthorized access to member information systems including appropriate reports to regulatory and law enforcement agencies. (III. C. 1.g)		
30	6h	(h) Measures to protect against destruction, loss, or damage of member information due to potential environmental hazards. (III. C. 1.h)		
31	7	Does the staff receive training to comply with the information security program? (III. C. 2)		
32	8	Are key controls, systems, and operating procedures for the information security program regularly tested? (III. C. 3)		
33	9	Does management have appropriate procedures to dispose of member information and consumer information? (III.C.4)		
34	10	Does the credit union effectively oversee critical service provider arrangements? (III. D)		
35	11	Does the credit union monitor, evaluate, and adjust the information security program, as needed? (III. E)		
36	12	Does management report to the board of directors, at least annually, on the overall status of the information security program and compliance with Part 748, Appendix A and B guidelines? (III. F)		
37		Section Rating:		
38		**Section C: Part 748 Appendix B - Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice**		
39	13	Has management developed and implemented a risk-based response program to address incidents of unauthorized access to member information?		
40	14	Is the program appropriate for the size and complexity of the credit union and the nature and scope of its activities?		
41	15	Does the program outline procedures to address incidents of unauthorized access to member information in systems maintained by its domestic and foreign service providers?		
42	16	Does the credit union's response program contain:		
43	16a	a) Procedures for assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed without permission?		

	A	B	D	F
5		**IT - 748 Compliance**		
6		**Objective: Ensure management has considered the requirements and guidelines related to information technology initiatives.**		
7		**Question**	**Yes/No/ NA/**	**Comment**
44	16b	b) Notifying the appropriate NCUA Regional Director, and, in the case of state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information?		
45	16c	c) Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing?		
46	16d	d) Appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information?		
47	16e	e) Notifying members when warranted?		
48	16f	f) Notification of affected members when the incident involves unauthorized access to member information systems maintained by a credit union's service providers?		
49	17	Does the member notice:		
50	17a	a) Provide information in a clear and conspicuous manner?		
51	17b	b) Describe the incident in general terms and the type of member information that was the subject of unauthorized access or use?		
52	17c	c) Describe what the credit union has done to protect the members' information from further unauthorized access?		
53	17d	d) Include a telephone number that members can call for further information and assistance?		
54	17e	e) Remind members of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the credit union?		
55	18	Does the member notice include the following when necessary:		
56	18a	a) A recommendation that the member review account statements and immediately report any suspicious activity to the credit union?		
57	18b	b) A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud?		
58	18c	c) A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted?		
59	18d	d) An explanation of how the member may obtain a credit report free of charge?		
60	18e	e) Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft?		
61	19	Are member notices delivered in a manner designed to ensure that a member can reasonably be expected to receive it?		

	A	B	D	F
5		**IT - 748 Compliance**		
6		**Objective: Ensure management has considered the requirements and guidelines related to information technology initiatives.**		
7		**Question**	**Yes/No/ NA/**	**Comment**
62		Section Rating:		
63		**Overall Questionnaire Comments:**		
64				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B8
Comment: The questions in Section A are requirements under R&R Part 748 Security Program.

Cell: B15
Comment: Vital records include at least the following
records, as of the most recent month-end:
(a) A list of share, deposit, and loan balances
for each member's account which:
(1) Shows each balance individually
identified by a name or number;
(2) Lists multiple loans of one account
separately; and
(3) Contains information sufficient to
enable the credit union to locate each member,
such as address and telephone number, unless
the board of directors determines that the
information is readily available from another
source.
(b) A financial report, which lists all of the
credit union's asset and liability accounts and
bank reconcilements.
(c) A list of the credit union's financial
institutions, insurance policies, and investments.
This information may be marked
''permanent'' and stored separately, to be
updated only when changes are made.

Cell: D17
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B18
Comment: The numbers at the end of a question are used to provide a reference to the sections in Appendix A "Guidelines for Safeguarding Member Information"

Cell: B19
Comment: Ensure that the board:
(a) approved the credit union's written information security policy and program;
(b) oversees the development, implementation, and maintenance of the information security program; and
(c) assigned specific responsibility for implementing the program and for reviewing management reports.

Cell: B20
Comment: The risk assessment process should:
(a) identify reasonably foreseeable internal and external threats;
(b) assess the likelihood and potential damage of those threats, taking into consideration the sensitivity of member information; and
(c) assess the sufficiency of controls including: policies, procedures, automated systems, and other arrangements.

Cell: B22
Comment: Based on the results of the risk assessment, did management address the following security issues/controls:

Cell: B23
Comment: Including controls to:
- authenticate and permit access only to authorized individuals
- controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means.

Cell: B31
Comment: A best practice is to require annual review and written acknowledgement (maintained in employee file) of information security training.

Cell: B32
Comment: The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests of key controls will normally be performed at least annually and whenever there are significant changes to critical systems, network configurations, or control processes. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs. Examples of tests may include vulnerability/security assessments, penetration tests, IT audits, internal audit reviews, etc.

Cell: B33
Comment: Measures for disposal procedures of member and consumer information should be approved by the Board of Directors, reviewed for potential risks, and properly manage and control the disposal process

Cell: B34
Comment: Has management:
(a) documented due diligence in selecting service providers;
(b) required that service providers implement appropriate measures by use of contractual service level agreements to meet the objectives of the security program;
(c) established a program to regularly monitor service provider activities and reports in order to verify that providers are satisfying their contractual obligations; and
(d) reviewed audits, summaries of test results, or other equivalent evaluations (e.g., SAS 70 & vulnerability tests) of service providers.

Cell: B35
Comment: The credit union should monitor, evaluate, and adjust the information security program, as appropriate, for:
(a) relevant changes in: technology, the sensitivity of its member information, and internal or external threats to information; and
(b) changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to member information systems.

Cell: B36

Comment: Management should keep the board informed and up to date on all IT related matters such as:
(a) risk assessment;
(b) risk management;
(c) control decisions;
(d) service provider arrangements;
(e) testing results;
(f) security breaches;
(h) identified violations and management's responses; and
(i) recommendations for changes in the information security program.

Cell: D37
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B38
Comment: Appendix B describes response programs, including member notification procedures, that a federally insured credit union should develop and implement to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member.

Cell: B40
Comment: A response program should be a key part of a credit union's information security program and should be developed in accordance with their risk assessment.

Cell: B41
Comment: A credit union's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to or use of the credit union's member information, including notification of the credit union as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

Cell: B44
Comment: Sensitive member information means:
a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account.
Sensitive member information also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

Cell: B46
Comment: example: monitoring, freezing, or closing affected accounts, while preserving records and other evidence;

Cell: B48
Comment: It is the responsibility of the credit union to notify the credit union's members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

Cell: B49
Comment: When member notification is warranted, a credit union may not forgo notifying its customers of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so.

Cell: B55
Comment: The notice should encourage the member to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.

Cell: B61
Comment: For example, the credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Cell: D62
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - Audit Program**		
6		**Objective: To determine whether e-Commerce activities are subject to regular, independent review (internal and/or external) and whether management is appropriately addressing significant matters resulting from such reviews.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8	1	Does the credit union have policies or procedures in place that describe how and when independent reviews of IT related areas will be performed?		
9	2	Do policies or procedures include any of the following external reviews:		
10	2a	(a) External Vulnerability Assessment?		
11	2b	(b) Penetration Testing? If yes, consider Pen Test Review Questionnaire.		
12	2c	(c) Assessment of IT department general controls?		
13	2d	(d) IT Risk Assessment to include Part 748, Appendix A?		
14	2e	(e) Security Assessment		
15	3	Does the internal audit program have a written audit plan that includes the following reviews:		
16	3a	(a) The risk assessment process?		
17	3b	(b) Employee & vendor access levels to critical systems?		
18	3c	(c) Employee compliance to IT & computer use policies?		
19	3d	(d) The vendor management process?		
20	3e	(e) SAS 70 (or service auditor's) reports and test whether "Client Control Considerations" are properly implemented by the applicable departments?		
21	4	Is adequate documentation of IT audits maintained?		
22	5	Is staffing sufficient in the internal audit department?		
23	6	Does the audit staff receive adequate IT training?		
24	7	Is the IT audit function independent and free from influence by management and/or departments that it audits?		
25	8	Does internal audit regularly report review activity and results to the Supervisory Committee?		
26	9	Are IT audit findings and summaries from independent assessments clearly communicated to management and the board for risk mitigation?		
27	10	Is a follow-up process in place to ensure that material findings and weaknesses are corrected?		
28		Section Rating:		
29		**Overall Questionnaire Comments:**		

	A	B	D	F
5		**IT - Audit Program**		
6		**Objective: To determine whether e-Commerce activities are subject to regular, independent review (internal and/or external) and whether management is appropriately addressing significant matters resulting from such reviews.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
30				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B8
Comment: In-house IT audits, by qualified auditors, should be performed on a periodic basis. When in-house audit expertise is inadequate and IT Risk is high, CUs should outsource to qualified third party auditors.

Cell: B10
Comment: A Vulnerability Assessment identifies weaknesses and vulnerabilities that pose risk to an organization and allows the organization to mitigate threats and take corrective action. The assessment is usually performed remotely. These assessments should be low cost and performed frequently (anywhere from weekly to quarterly).

Cell: B11
Comment: A Penetration Test is a consultant attempting to hack your system to test the security. These tests are more extensive and costly than a vulnerability assessment.

Cell: B12
Comment: These reviews includes general IT controls and operating policies and procedures. They are obtained less frequently, possibly every 1-2 years or after a major systems change.

Cell: B15
Comment: The plan should cover at least the next 12 months and be approved by the supervisory committee.

Cell: B19
Comment: The CU should assign a person responsible for due diligence monitoring. Internal audit can serve as a central repository for this information and ensure ongoing compliance with vendor management policies.

Cell: B20
Comment: There are two types of service auditor's reports: a Type I report provides the service organization's description of controls at a specific point in time, and the auditor's opinions as to whether the description is presented fairly and whether the controls are suitably designed to achieve the related control objectives; a Type II report includes all of the elements of the Type I report as well as actual testing of the controls to determine whether they are operating with sufficient effectiveness to achieve the related control objectives.

Cell: B21
Comment: There should be policies addressing work paper retention and maintaining support for all audit findings and

work performed.

Cell: B22
Comment: Staff performing IT audits should have information's systems knowledge commensurate with the scope and sophistication of the IT environment.

Cell: B23
Comment: Professional development programs should be in place for audit staff to maintain the necessary technical expertise.

Cell: D28
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - Authentication**		
6		**Objective: To determine whether the credit union has implemented authentication techniques to ensure the adequate protection of credit union and member data at all times.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8		**Section A: Member Authentication**		
9	1	Are members required to authenticate themselves through the use of unique PINs or passwords?		
10	2	Does the credit union use multifactor authentication, layered security, or other controls reasonably calculated to mitigate the risk associated with Internet-based products and service to their members?		
11	3	Are members electronically identified using a:		
12	3a	(a) Static IP address?		
13	3b	(b) Dynamic Host Configuration Protocol (DHCP)?		
14	4	Has management implemented adequate procedures to ensure the proper identification of a member before resetting or reissuing a password or PIN?		
15		Section Rating:		
16		**Section B: Strong Authentication**		
17	5	Is authentication data (usernames, passwords, PINs, etc.) encrypted in the database residing on the authentication server?		
18	6	Is authentication data (usernames, passwords, PINs, etc.) encrypted during transmission?		
19	7	Are there any systems or web applications that use One Time passwords or password that have a short life?		
20	8	Is authorized access to sensitive data (such as member accounts or personnel records) logged?		
21	9	Are the logs regularly reviewed to determine whether the access and use of such data was appropriate?		
22		Section Rating:		
23		**Section C: Biometric Devices**		
24	10	Has a risk assessment or cost/benefit analysis been performed with regards to the implementation of biometrics?		
25	11	Does the credit union use biometrics devices for authentication purposes? If no, skip the remainder of this section.		
26	12	Are tolerance levels and policies in place that ensure that the user authentication process is performed correctly?		
27	13	Are statistical performance metrics routinely monitored to ensure that the process is performed correctly?		
28		Section Rating:		
29		**Section D: Encryption Keys**		
30	14	Are there policies and procedures in place that describe how and when encryption should be used to protect the following transmitted and stored information:		
31	14a	(a) Key management?		
32	14b	(b) Key distribution (issuance, revocation, re-issuance)?		

	A	B	D	F
5		**IT - Authentication**		
6		**Objective: To determine whether the credit union has implemented authentication techniques to ensure the adequate protection of credit union and member data at all times.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
33	14c	(c) Key storage (on a server with no connection to outside networks)?		
34	15	If there are international implications, has the credit union put safeguards in place to ensure compliance with US government policies and restrictions associated with the exportation of encryption technology?		
35		Section Rating:		
36		**Section E: Digital Signatures**		
37	16	Does the credit union use digital signatures? If no, skip this section.		
38	17	Are there policies and procedures in place which describe how and when digital signatures should be used to ensure member, credit union, or transaction authenticity? Considerations include:		
39	17a	(a) Are digital signatures issued, managed, and/or certified by an external vendor?		
40	17b	(b) Are there procedures dealing with the issuance, renewal and revocation of certificates?		
41	18	Are digital signatures used to authenticate the credit union?		
42	19	Are digital signatures used to authenticate the members?		
43	20	Are digital signatures used to authenticate member transactions?		
44	21	Does digital signature procedures include the following:		
45	21a	(a) Logging sessions?		
46	21b	(b) Generating and auditing session reports?		
47	21c	(c) Following up on unusual session activity or errors?		
48	22	Are current laws being monitored with respect to changes governing the use of digital signatures?		
49		Section Rating:		
50		**Section F: Certificate Authorities (CA)**		
51	23	Does the credit union function as a certificate authority? If no, skip this section.		
52	24	Has the credit union performed due diligence with respect to the legal implications of providing a CA function?		
53	25	Have CA limitations been established for:		
54	25a	(a) Number of transactions?		
55	25b	(b) Transaction types?		
56	25c	(c) CA expirations?		
57	26	Does the credit union provide adequate protection for the servers housing the CA information and directories?		
58	27	Does the credit union conform to CA standards established by the Internet Engineering Task Force (IETF) and National Institute of Science and Technology (NIST)?		
59	28	Are the hosting certificates properly procured and stored?		

	A	B	D	F
5		**IT - Authentication**		
6		**Objective: To determine whether the credit union has implemented authentication techniques to ensure the adequate protection of credit union and member data at all times.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
60	29	Does the credit union maintain backup copies of the certificates?		
61	30	Are backup copies properly secured against unauthorized access or use?		
62		Section Rating:		
63		***Section G: Risk Assessment***		
64	31	Does the credit union have a written risk assessment regarding the implementation of appropriate authentication methodologies?		
65	32	Does the credit union have an ongoing process to review authentication technology and ensure appropriate changes are implemented?		
66	33	Does the credit union use single-factor authentication tools?		
67		Section Rating:		
68		**Section H: Member Account Verification**		
69	34	Does the credit union accept new members through the Internet or other electronic channels?		
70		Section Rating:		
71		**Section I: Monitoring and Reporting**		
72	35	Does the credit union use audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities?		
73	36	Does the credit union use reporting mechanisms to inform security administrators when users are no longer authorized to access a particular application / system and to permit the timely removal or suspension of user account access?		
74		Section Rating:		
75		**Section J: Member Awareness**		
76	37	Does the credit union have in place a member awareness program to educate your members against fraud and identity theft?		
77		Section Rating:		
78		**Overall Questionnaire Comments:**		
79				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B9
Comment: Authentication is a method by which to identify and verify that a member is who they portend to be. Authentication methodologies generally involve three basic "factors": (1)something the user knows (e.g., password, PIN); (2)something the user possesses (e.g., ATM card, smart card); and (3)something the user is (e.g., biometric characteristic, such as a fingerprint or retinal pattern).

Cell: B10
Comment: The FFIEC issued guidance on Authentication in an Internet Banking Environment. The FFIEC agencies consider single-factor authentication to be inadequate for high-risk transaction involving access to customer information or movement of funds to other parties.

Cell: B11
Comment: An IP address is a 32-bit number (Numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.) that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note too. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received. An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself - that is, between the routers that move packets from one point to another along the route - only the network part of the address is looked at.

Recording the IP address will help provide an audit trail should it be necessary for authorities to trace an intrusion. FYI, Dynamic Host Configuration Protocol (DHCP) does not use a dedicated address 100% of the time, which is more efficient and may be more secure. While the path of the DHCP address can and will change, the static IP address is constant and will not change, making it more susceptible to unauthorized intrusion attempts.

Cell: B12
Comment: An IP address assigned to a computer which does not change unless changed by a person, such as an administrator. This method of identification can be easily spoofed unless additional safeguards such as MAC (Media Access Control, generally used for wireless access) filtering are also employed.

Cell: B13
Comment: An Internet protocol which provides for automated allocation, configuration, and management of IP addresses. IP addresses are assigned to a computer when the user initiates a session rather than having an IP address permanently assigned to the computer.

Cell: B14
Comment: Secondary authentication methods might include giving a mother's maiden name, providing a code word or phrase, or sending the PIN to the member's mailing address on file.

Cell: D15
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B17
Comment: Should an unauthorized individual gain access to the authentication server, encrypting user authentication credentials would prevent that individual from using those credentials for fraudulent purposes.

Cell: B19
Comment: Cracking short-lived passwords is extremely difficult to do; thereby enhancing security. However, managing short-term passwords is a more difficult process (i.e. distributing those passwords security to the end users).

Cell: B20
Comment: Virtually all systems (hardware and software) have the capability to log transactions or events. Such logs should be enabled in order to capture and track who accessed the system, what they did, when they did it, and how it was done. This information is useful for forensic purposes as well as for ensuring compliance with established policies and procedures.

Cell: B21
Comment: One or more individuals should be assigned to review log files. Such reviews can help identify unauthorized access and/or use on a timely basis.

Cell: D22
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B24
Comment: Biometric devices consist of retina, fingerprint scanners, face scanners, etc.

Cell: D28
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B34
Comment: Management should understand that US policy is still evolving with respect to allowing the export of 128-bit (vs. 56-bit) encryption products to certain countries. For example, if a member service representative receives a request from a member that is in a foreign country for assistance in obtaining Internet browser software that allows 128-bit encryption to facilitate secure Internet banking, the credit union should consult with legal counsel to ensure it does not violate US law in trying to assist the member.

More information concerning federal laws on encryption can be found on the U.S. Department of Commerce, Bureau of Industry and Security's (BIS) website at: http://www.bxa.doc.gov/Encryption/regs.htm.

Cell: D35
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B37
Comment: A digital signature is designed to be a convenient, time-saving, and secure way of signing electronic documents. Digital signatures (unique identifying marks generated by computers and attached to electronic documents) are increasingly being used to authenticate e-mail and contractual arrangements made over the

Internet. Digital signatures use what is known as "public key cryptography," which employs an algorithm using two different but mathematically related "keys"; one for creating a digital signature or transforming data into a seemingly unintelligible form, and another for verifying a digital signature or returning the message to its original form. This technology requires the use of one or more trusted third parties to associate an identified signer with a specific public key. That trusted third party is referred to as a "certification authority". (See next section for definition of certificate authority.)

Cell: B48
Comment: Although recent laws have been passed regarding the use of and protections provided with respect to digital signatures, this is an area that will probably continue to require close attention. Management should consult with legal counsel on an ongoing basis to ensure compliance with applicable laws.

Cell: D49
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B51
Comment: Certificate Authorities are entities that create, issue, and maintain certificates which identify users (i.e. credit union and members) and authenticate them to each other during electronic exchanges. To authenticate two parties, a certificate authority issues a certificate (an electronic record which lists a public key as the "subject" of the certificate and confirms that the individual identified in the certificate holds the corresponding private key). The individual identified in the certificate is termed the "subscriber. A certificate's principal function is to bind a key pair with a particular subscriber. A "recipient" of the certificate desiring to rely upon the authenticity of the subscriber named in the certificate (whereupon the recipient becomes a "relying party") can use the public key listed in the certificate to verify that the subscriber created the corresponding private key. If such verification is successful, this chain of reasoning provides assurance that the corresponding private key is held by the subscriber named in the certificate, and that the message, e-mail, contract, digital signature, etc. was created by that particular subscriber.

Cell: D62
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B64
Comment: The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the credit union's internet banking systems. The risk should be evaluated in light of the type of member; the member transactional capabilities; the sensitivity of the member information being communicated to both the credit union and the member; the ease of using the communication method; and the volume of transactions.

Cell: B65
Comment: An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the credit union's internet-based products and services. The level of authentication used by a credit union in a particular application should be commensurate to the level of risk in that application.

Cell: B66
Comment: Single-factor authentication tools includes passwords, PINs. The credit union should assess the adequacy of such authentication technique in light of new or changing risks such as phishing, pharming, malware and the evolving sophistication of compromise techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, credit unions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. (Refer to FFIEC Guidance "Authentication in an Internet Banking Environment").

Cell: D67
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B69
Comment: With the growth in e-commerce, credit unions should use reliable methods of originating new member accounts online. Moreover, member identity verification during account origination is required by section 326 of the USA Patriot Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions.

Cell: D70
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B72
Comment: The activation and maintenance of audit logs can help credit unions to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. Suspicious activities should be reported to NCUA and FINCEN as required by the Bank Secrecy Act.

Cell: B73
Comment: If your critical systems or processes are outsourced to third parties, you should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to the credit union in a timely manner.

Cell: D74
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B76
Comment: Credit Unions should evaluate their member education efforts to determine if additional steps are necessary. The member awareness program should be periodically evaluated for effectiveness. Methods to evaluate a program's effectiveness include tracking the number of members who report fraudulent attempts to obtain their authentication credentials (e.g. ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

Cell: D77
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - Business Continuity Planning (BCP)**		
6		**Objective: To determine if an adequate BCP exists which will minimize the risk of service outages in the event of a disaster or point of failure along service delivery channels.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8		**Section A: General**		
9	1	Has management established and documented a Business Continuity Plan to ensure that all systems, (including essential non-systems) and related business processes can be recovered in a timely manner?		
10	2	Does the credit union's business continuity and/or disaster recovery plan (BCP/DRP) address the timely recovery of its IT functions in the event of a disaster?		
11	3	Is the BCP/DRP appropriate for the size and complexity of the credit union?		
12	4	Does the plan identify critical plan personnel, their backups, a command center site, and an alternate command site?		
13	5	Are critical business functions identified and prioritized?		
14	5a	Is the BCP/DRP tested periodically, and what was the date of the last test?		
15	6	Has the credit union performed a Business Impact Analysis (BIA)?		
16	7	Has management established maximum allowable down times for the critical business functions identified above?		
17	8	Does management review its plan at least annually or whenever there are significant changes in the technology, infrastructure, or IT Services of the CU?		
18	9	Has the credit union ever invoked its disaster recovery plan?		
19	10	If so, was the plan modified based upon lessons learned?		
20	11	Does the BCP/DRP take into consideration those services provided by outsourced vendors?		
21		Section Rating:		
22		**Section B: Backup And Recovery**		
23	12	Has management established appropriate backup policies and procedures to ensure the timely restoration of critical services?		
24	13	Are BCP and recovery procedures maintained at the alternate site and off-site storage locations in a secured manner?		
25	14	Is security at the recovery site adequately addressed?		
26	15	Does management schedule the backup and retention of data as well as the erasure and release of media when retention is no longer required?		
27	16	Are updated hardware and software inventories maintained, including version numbers for software?		
28		Section Rating:		
29		**Section C: Backup Power**		

	A	B	D	F
5		**IT - Business Continuity Planning (BCP)**		
6		**Objective: To determine if an adequate BCP exists which will minimize the risk of service outages in the event of a disaster or point of failure along service delivery channels.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
30	17	Does the credit union have adequate uninterruptible power supply (UPS) protection to perform an orderly systems shutdown in case of power loss?		
31	18	Has management ensured that critical systems are connected to a backup power source?		
32	19	Are backup power sources periodically tested?		
33		Section Rating:		
34		**Section D: Incident Response**		
35	20	Does the credit union have incident response policies and procedures that are based upon the criticality of the incident?		
36	21	Do the incident response procedures address the loss of service due to cyber crimes?		
37	22	Have incident response procedures ever been invoked?		
38	23	Does the BCP/DRP include a provision to notify the NCUA Regional Director within 5 business days of a catastrophic act and filing a Catastrophic Act Report (CAR) within a reasonable timeframe? (NCUA 748.1B)		
39		Section Rating:		
40		**Overall Questionnaire Comments:**		
41				

Cell: B2

Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3

Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: B6

Comment: Business Continuity is inclusive of disaster recovery and addresses the needs for additional planning.

Cell: D7

Comment: The only data entry in the yellow cells should be Yes, No, NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B9

Comment: Business continuity planning, which encompasses disaster recovery planning, is a process of information gathering and analysis that results in an integrated strategy and corresponding plan to respond to an unplanned interruption in normal business operations. The ultimate objective of this process is to provide timely availability of all systems and non-systems related resources necessary to operate critical business processes at a level acceptable to management. Typically, critical business processes include the credit union's core activities (e.g., branch operations and customer service) that contribute directly to the goals of the credit union. In the event of an unplanned interruption to normal business operations, degraded levels of service may be acceptable for some period of time. Essential non-systems are not tied to the network itself, such as time lock safes, heating, air conditioning, alarms, but are important to operations.

Cell: B11

Comment: The business continuity/disaster recovery plan BCP/DR should be commensurate with the size and complexity of the credit union. If the credit union relies heavily on internet, web, or electronic services and communications to conduct business, then the BCP/DR plans should address all appropriate delivery avenues. The plan should address at a minimum:
a) the timely recovery of services in the event of a disaster or other event that causes the system to be down;
b) environmental risks (i.e. flood, earthquakes, hurricane, fire, etc.) when determining the location of alternate processing sites;
c) alternate communication methods and paths; and
d) alternate service providers

Cell: B15

Comment: A credit union's first step in developing a BCP is to perform a business impact analysis. Management should determine possible threats to the credit union's business continuity. Threats vary with each credit union's unique situation. Examples of threats include, but are not limited to:

- Terrorism;
- Power failure;
- Equipment failure;
- Fire;
- Theft;
- Flood; and
- Employee sabotage.

The amount of time and resources spent on performing the BIA will depend on the size and complexity of the credit union. The BIA should include all business functions and departments, not just data processing. Management should identify critical business functions and prioritize them. It should estimate the maximum allowable downtime for critical business processes and the costs associated with that downtime.

Cell: B16
Comment: A detailed schedule should be developed to establish acceptable timelines for restoring each critical system after a failure event (either on-site or at a remote location.)

Cell: B17
Comment: Business continuity plans should be tested annually. The results should be documented and analyzed to identify necessary changes.

Cell: B20
Comment: Management's business continuity planning (and testing) efforts should address vendor notification procedures, alternate connectivity, etc. and the parties responsible for performing these tasks.

Cell: D21
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B23
Comment: Backup and recovery policies should include

- systems to be backed up
- method and type of backup
- frequency of backup
- storage and encryption of backup media
- rotation schedule
- restoration procedures
- testing

Cell: B25
Comment: The recovery facility should exhibit a greater level of security protection than the primary operations site since the people and systems controlling access to the recovery site will not be as familiar with the relocated personnel using it.

Cell: B26
Comment: In a computer environment, a credit union's significant records are typically archived by making copies of databases or data files and retaining these "backups". It is important that the completion of the backup process is logged and that management review these logs. The policies, procedures, standards, and

guidance regarding management's review of backup logs typically include:

- frequency of review;
- assignment of responsibility;
- documentation produced during backup process; and
- assessment of successful and timely backup.

Backup policies, procedures, standards, and guidance should be followed to ensure the availability of data significant to the credit union's operations.

Cell: B27
Comment: The best practice is to update software inventories at least quarterly and hardware inventories continuously.

Cell: D28
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B30
Comment: UPS is a power supply that includes a battery to maintain power in the event of a power outage. Typically, a UPS keeps a computer running for several minutes after a power outage, enabling you to save data and shut down the computer systematically. Many UPSs offer a software component that enables an automated backup and shut down procedures in case there's a power failure while you're away from the computer. There are two basic types of UPS systems: standby power systems (SPSs) and on-line UPS systems. An SPS monitors the power line and switches to battery power as soon as it detects a problem. The switch to battery, however, can require several milliseconds, during which time the computer is not receiving any power. Standby Power Systems are sometimes called Line-interactive UPSs.

Cell: D33
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B38
Comment: The CAR should include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiency(ies)) might have contributed to the catastrophic act; and what has been done or is planned to be done to correct the deficiency(ies)).

Cell: D39
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - Compliance**		
6		**Objective: Ensure management has considered the requirements and guidelines related to information technology initiatives.**		
7		**Question**	**Yes/No/ NA/ NR**	**Comment**
8		**Section A: Part 749 - Records Preservation Program**		
9	1	Has the board of directors established a written vital records preservation program consistent with the regulation? (749.2)		
10	2	Does management maintain a records preservation log showing what records were stored, where the records were stored, when the records were stored, and who sent the records for storage? (749.2)		
11	3	Are vital records maintained in a format that accurately reflects the information, remains accessible to all persons who are entitled to access, and is capable of being reproduced by transmission, printing, or otherwise? (749.5)		
12	4	Has the board of directors approved a schedule authorizing the disposal of certain records on a continuing basis? (Appendix A)		
13	5	Does the credit union prepare an index of records destroyed and retain the index permanently? (Appendix A)		
14	6	Is the destruction of records carried out by at least two persons and are their signatures affixed to the listing attesting to the fact that records were actually destroyed? (Appendix A)		
15	7	Do policies identify official and key operational records that should not be destroyed. (Appendix A)		
16		Section Rating:		
17		**Section B: Website Compliance**		
18	8	If the credit union provides privacy disclosures on their website, are they: clear and conspicuous, reasonably understandable, and designed to call attention to the nature and significance of the information in the notice? (716.3)		
19	9	Does the Internet disclosure use text or visual cues to encourage scrolling down the page to view the entire notice and ensure that other elements on the website do not distract attention from the notice? (716.3)		
20	10	Is the privacy notice, or a link to that notice, on a screen which is frequently accessed by members (e.g. homepage) or a page on which transactions are conducted? (716.3)		

	A	B	D	F
5		**IT - Compliance**		
6		**Objective: Ensure management has considered the requirements and guidelines related to information technology initiatives.**		
7		**Question**	**Yes/No/ NA/ NR**	**Comment**
21	11	Does the credit union display the official NCUA insurance sign on its home page and any page where it accepts deposits or opens accounts? (740.4)		
22	12	If the credit union conducts real estate lending, is the "Equal Housing Lender" logo present on each Internet page where real estate-related loans are advertised? (NCUA 701.31)		
23	13	If new members are approved over the website, is member identity properly verified? (NCUA 748.2)		
24	14	Does the credit union post its share and/or loan rates on the website? If no, skip the rest of this section.		
25	14a	(a) Is the "annual percentage yield" for shares disclosed using this term? (Reg DD)		
26	14b	(b) Is an effective or expiration date disclosed on the advertised APY? (Reg DD)		
27	14c	(c) Is the "annual percentage rate" or "APR" for loans disclosed using one or both of these terms? (Reg. Z)		
28	14d	(d) Is the APR on credit cards disclosed in at least 18-point font? (Reg. Z(b)(1))		
29		Section Rating:		
30		**Section C: Letter 03-CU-08 - Web linking Guidance**		
31	15	Have due diligence reviews been performed on third parties with which the credit union has web linking relationships?		
32	16	Are written agreements in place for significant web linking partners?		
33	17	Are clear and conspicuous webpage disclosures provided to explain the credit union's limited role and responsibility with respect to products and services offered through linked third-party websites?		
34	18	Does the credit union have procedures for responding to complaints from members regarding linked websites?		
35		Section Rating:		
36		**Overall Questionnaire Comments:**		
37				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B9
Comment: The vital records preservation program must contain procedures for storing duplicate vital records at a vital records center and must designate the staff member responsible for carrying out the vital records duties. Records must be stored every 3 months, within 30 days after the end of the 3-month period.

Cell: B10
Comment: Credit unions, which have some or all of their records maintained by an off-site data processor, are considered to be in compliance for the storage of those records.

Cell: B11
Comment: Formats include, but are not limited to: paper originals, machine copies, micro-film or fiche, magnetic tape, or any electronic format that accurately reflects the information in the record.

Cell: B12
Comment: A system for disposal of records eliminates the need for board approval each time the credit union wants to dispose of the same types of records created at different times. Record destruction may impact the credit union's legal standing to collect on loans or defend itself in court. Since each state can impose its own rules, it is prudent for a credit union to consider consulting with legal counsel when setting minimum retention periods. A record pertaining to a member's account that is not considered a vital record may be destroyed once it is verified by the supervisory committee. Records, for a particular period, should not be destroyed until both a comprehensive annual audit by the supervisory committee and a supervisory examination by the NCUA have been made for that period. Records that may be periodically destroyed include:
(a) Applications of paid off loans.
(b) Paid notes.
(c) Various consumer disclosure forms, unless retention is required by law.
(d) Cash received vouchers.
(e) Journal vouchers.
(f) Canceled checks.
(g) Bank statements.
(h) Outdated manuals, canceled instructions, and nonpayment correspondence from the NCUA and other governmental agencies.

Cell: B14
Comment: Dual oversight reduces the risk that confidential member or credit union data is stolen. Records should be destroyed in a manner that renders them unrecoverable and unreadable.

Cell: B15

Comment: Official records of the credit union that should be retained permanently are:
(a) Charter, bylaws, and amendments.
(b) Certificates or licenses to operate under programs of various government agencies, such as a certificate to act as issuing agent for the sale of U.S. savings bonds.
(c) Current manuals, circular letters and other official instructions of a permanent character received from the NCUA and other governmental agencies.

Key operational records that should be retained permanently are:
(a) Minutes of meetings of the membership, board of directors, credit committee, and supervisory committee.
(b) One copy of each NCUA 5300 financial report or its equivalent.
(c) One copy of each supervisory committee comprehensive annual audit report and attachments.
(d) Supervisory committee records of account verification.
(e) Applications for membership and joint share account agreements.
(f) Journal and cash record.
(g) General ledger.
(h) Copies of the periodic statements of members, or the individual share and loan ledger. (A complete record of the account should be kept permanently.)
(i) Bank reconcilements.
(j) Listing of records destroyed.

Cell: D16

Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B18

Comment: (a) A Notice is reasonably understandable if you:
(1) Present the information contained in the notice in clear, concise sentences, paragraphs and sections;
(2) Use short, explanatory sentences or bullet lists whenever possible;
(3) Use definite, concrete, everyday words and active voice whenever possible;
(4) Avoid multiple negatives;
(5) Avoid legal and highly technical business terminology wherever possible; and
(6) Avoid explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. You design your notice to call attention to the nature and significance of the information in it if you:
(1) Use a plain-language heading to call attention to the notice;
(2) Use a typeface and type size that are easy to read;
(3) Provide wide margins and ample line spacing;
(4) Use boldface or italics for key words; and
(5) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars.

Cell: B20

Comment: Links must be labeled appropriately to convey the importance, nature, and relevance of the notice.

Cell: B21

Comment: To ensure its legibility, the official sign shall be depicted as shown in the regulation. Electronic insurance signs may be obtained from the NCUA.GOV website. If the sign is reduced on the web page affecting the legibility, popup technology should be employed to allow users to view a legible version.

Cell: B23

Comment: 748.2 requires compliance with 31 CFR 103.121(b)24)(ii)(B) Verification through non-documentary methods. For a credit union relying on non-documentary methods, the CIP must contain procedures that describe the

non-documentary methods the credit union will use. (1) These methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.

Cell: D29
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B30
Comment: A web link is a word, phrase, or image that contains coding that will transport the viewer to a different part of the website or a completely different website by clicking on it.

Cell: B31
Comment: A credit union should conduct sufficient due diligence to determine whether it wishes to be associated with the quality of products, services, and overall content provided by third-party sites. A credit union should consider more product focused due diligence if the third parties are providing financial products, services, or other financial website content. In this case, customers may be more likely to assume the institution reviewed and approved such products and services. In addition to reviewing the linked third-party's financial statements and its customer service performance levels, a credit union should consider a review of the privacy and security policies and procedures of the third party. Also, the credit union should consider the character of the linked party by considering its past compliance with laws and regulations and whether the linked advertisements might by viewed as deceptive advertising in violation of Section 5 of the Federal Trade Commission Act.

Cell: B32
Comment: The credit union should consider including contract provisions to indemnify itself against claims by: (1) dissatisfied purchasers of third-party products or services; (2) patent or trademark holders for infringement by the third party; and (3) persons alleging the unauthorized release or compromise of their confidential information, as a result of the third-party's conduct. The agreement should not include any provision obligating the credit union to engage in activities inconsistent with the scope of its legally permissible activities. The agreement should include conditions for terminating the link.

Cell: B33
Comment: The level of detail of the disclosure and its prominence should be appropriate to the harm that may ensue from customer confusion inherent in a particular link. The credit union might post a disclosure stating it does not provide, and is not responsible for, the product, service, or overall website content available at a third-party site. It might also advise the member that its privacy polices do not apply to linked websites and that a viewer should consult the privacy disclosures on that site for further information. The conspicuous display of the disclosure, including its placement on the appropriate webpage, by effective use of size, color, and graphic treatment, will help ensure that the information is noticeable to members.

Cell: D35
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - Firewalls**		
6		**Objective: To evaluate whether the firewall environment has been designed to adequately support the network infrastructure within the credit union and whether day-to-day operations promotes the integrity of the firewalls in place.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8	1	Has the credit union performed a risk assessment to determine the need for firewalls?		
9		**Section A: Firewall Policy**		
10	2	If the risk assessment indicated a firewall is needed, has management installed a firewall? If no, skip this questionnaire.		
11	3	Does the credit union have a firewall policy? If no, skip to section B.		
12	4	Does the policy address:		
13	4a	(a) Who is responsible for managing the firewall?		
14	4b	(b) Who has access to the firewall?		
15	4c	(c) Who is responsible for the configuration (rules, ports, blocked sites, etc.) which establishes traffic permitted into and out of the firewall?		
16	4d	(d) Rules change procedures which include approval process, documentation retention, and verification process?		
17	4e	(e) Who is responsible for the retention of firewall rules?		
18	4f	(f) Firewall software patch management process including who is responsible, patch management notification process, documentation requirements, etc.?		
19	4g	(g) How often the configurations (rules, ports, etc.) are reviewed, who is responsible for the review, and how documentation for the review is retained?		
20	4h	(h) Who is responsible to monitor the firewall logs, the frequency of the review, and review documentation retained?		
21	4i	(i) The firewall backup procedure and testing of backups?		
22	4j	(j) Staff training requirements for proper firewall management?		
23		Section Rating:		
24		**Section B: Firewall Operation**		
25	5	Are passwords to access the firewall properly safeguarded?		
26	6	Is the firewall located in a controlled access area?		
27	7	Is the firewall properly placed to protect the credit union's assets?		
28	8	Are there any redundancies in the firewall configuration?		

	A	B	D	F
5		**IT - Firewalls**		
6		**Objective: To evaluate whether the firewall environment has been designed to adequately support the network infrastructure within the credit union and whether day-to-day operations promotes the integrity of the firewalls in place.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
29	9	Does the firewall run on a hardware appliance (e.g., Nokia)?		
30	10	Does the firewall run under a general purpose operating system (OS), e.g., Solaris, NT?		
31	11	Are the following types of firewalls in use?		
32	11a	(a) Packet Filtering		
33	11b	(b) Application Proxy		
34	11c	(c) Stateful Inspection		
35	11d	(d) Other (list)		
36	12	Do implemented firewalls detect and protect against:		
37	12a	(a) IP spoofing attacks?		
38	12b	(b) Denial of Service attacks?		
39	12c	(c) Programs like finger, whois, tracert and nslookup?		
40	13	Is the firewall operating system updated regularly?		
41	14	Are patches up to date?		
42	15	Is there a maintenance contract on the firewall?		
43	16	Are automated alerts in place?		
44	17	Are firewall logs reviewed?		
45	18	Is the review at least each business day?		
46	19	Are the firewall logs maintained for a specified period of time?		
47	20	Are firewall logs backed up?		
48	21	Is the firewall rule change control process automated?		
49	22	Do the firewall rules conform with corporate policy?		
50	23	Do they limit access to specific ports and services?		
51	24	Is there a default deny rule?		
52	25	Is the firewall backed up?		
53	26	Are backups safeguarded?		

	A	B	D	F
5		**IT - Firewalls**		
6		**Objective: To evaluate whether the firewall environment has been designed to adequately support the network infrastructure within the credit union and whether day-to-day operations promotes the integrity of the firewalls in place.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
54	27	Can the firewall be quickly reconfigured from backups (e.g., to restore a previous configuration)?		
55	28	Is backup recovery of the firewall tested at least annually?		
56	29	Is the firewall on an Uninterruptible Power Supply (UPS)?		
57	30	Are scans periodically run against the firewall to identify open ports and services?		
58	31	If external penetration tests are attempted after a major system update:		
59	31a	(a) Did the last test result in a favorable rating?		
60	31b	(b) Did management take corrective action on the recommendations from the penetration test results?		
61	32	Can the firewall be accessed by a secondary IT Committee or assigned staff member in an emergency?		
62		Section Rating:		
63		**Section C: Third Party Vendor**		
64	33	Do non-corporate personnel or vendors access the firewall? If no, skip to Section D.		
65	34	If so, have contracts with this vendor been reviewed by corporate legal personnel?		
66	35	Do access control limits limit access to specific static external IP addresses in the case of remote vendor support?		
67	36	Is all access by encrypted channel (e.g., SSH)? Exception: terminals directly connected to the firewall do not require a encrypted channel.		
68	37	If the firewall product uses a remote management architecture (e.g., Checkpoint management module and firewall module), are the controls adequate?		
69		Section Rating:		
70		**Section D: Audit**		
71	38	Is there an audit trail of who accesses the firewall administrative accounts?		
72	39	Is the log of administrative access printed, reviewed, and retained by management?		
73	40	Are firewall rules, policies, and procedures reviewed at least annually by a qualified auditor?		
74	41	Is each rule documented sufficiently to allow for review by a qualified auditor?		
75	42	Is there an audit trail of changes made during the past year?		
76		Section Rating:		
77		**Overall Questionnaire Comments:**		

	A	B	D	F
5		**IT - Firewalls**		
6		**Objective: To evaluate whether the firewall environment has been designed to adequately support the network infrastructure within the credit union and whether day-to-day operations promotes the integrity of the firewalls in place.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
78				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B8
Comment: Officials should assess the risks of their systems to evaluate the need to install firewalls. If internal systems are connected to the external world, firewalls should be deployed for risk mitigation purposes.

Cell: B19
Comment: You should actively monitor the configurations to identify changes that have occurred. Configurations need to be updated with any new services, installs, security breaches, anomalies in log reviews, etc.

Cell: D23
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B28
Comment: Such as, if the Internet Banking Server is located in a DMZ, is there a firewall on each side of the DMZ.

Cell: B30
Comment: Operating systems that are not primarily geared for IP networking tend to be more problematic, as more mature operating systems for IP networking have had time to find and eliminate their bugs. An attacker can often make the target equipment continuously reboot, crash, lose the ability to talk to the network, or replace files on the machine.

Cell: B32
Comment: Packet-level firewalls examine all data traveling between the local LAN and the Internet. Using a preprogrammed set of rules, packet filtering determines whether a packet is authorized based on its source and destination IP addresses.

Cell: B33
Comment: Proxy based firewalls stand between the Internet and a private network, and communicate with the Internet on the private network's behalf. When you configure a browser to use a proxy, the firewall passes a request from the browser to the Internet, then relays the Internet server's reply back to the browser. Proxy servers allow or restrict network access.

Cell: B34
Comment: This firewall type remembers information, such as source and destination addresses and port numbers, in a packet known to be legitimate. It uses this information to compare the "friendly" packet to the packet in question.

Cell: B37
Comment: Spoofing is a form of social engineering used by unauthorized users to assume the identity of an authorized user in an attempt to gain access to a system or account information.

Cell: B38
Comment: Denial of Service attacks threaten the ability of credit unions to provide Internet services due to flooding. Flooding refers to sending many requests to a server, generally causing the server processing time to increase or crashing the server. Denial of Service attacks can be protected with limitations.

Cell: B39
Comment: Finger is a UNIX command widely used on the Internet to find out information about a particular user, such as telephone number, whether currently logged on or the last time logged on. The person being "fingered" must have placed his or her profile on the system. Profiles can be very elaborate either as a method of social introduction or to state particular job responsibilities. Fingering requires entering the full user@domain address.

Whois is an Internet utility used to query a host and find out if a certain user is registered on that system. Originally developed by the military, others followed with their own whois databases, which provide a white pages directory for the organization.

Tracert is used to visually see a network packet being sent and received and the amount of hops required for that packet to get to its destination.

Nslookup is a MS-DOS utility that enables a user to look up an IP address of a domain or host on a network.

Cell: B48
Comment: This question pertains to a credit union that is using more than one firewall. If a rule is changed, can it update all firewalls automatically from a central location?

Cell: B51
Comment: The level of security you establish will determine how many threats can be stopped by your firewall. The highest level of security would be to simply block everything. Obviously that defeats the purpose of having an Internet connection. But a common rule of thumb is to block everything, then begin to select what types of traffic you will allow. You can also restrict traffic that travels through the firewall so that only certain types of information, such as e-mail, can get through. By default, all (enabled) Deny/Block rules should be logged in the firewall event log.

Cell: D62
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B66
Comment: How is remote access for the firewall restricted by management?

Cell: D69
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: D76

Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - IDS / IPS**		
6		**Objective: To evaluate whether the credit union is adequately securing its network environment with an Intrusion Detection System and/or Intrusion Prevention System to detect potentially harmful network activity.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8	1	Does the CU have an intrusion detection/prevention system (IDS/IPS)? If no, skip this questionnaire.		
9		**Section A: Policies**		
10	2	Are there policies and procedures in place to address intrusion detection?		
11	3	Do intrusion detection policies and procedures address escalation procedures?		
12	4	Do intrusion detection policies and procedures address how and when to file a Suspicious Activity Report (Required by NCUA Ltr. #96-CU-3)?		
13		Section Rating:		
14		**Section B: Operations**		
15	5	Is the system:		
16	5a	(a) Network-based		
17	5b	(b) Host-based		
18	6	Does the system reside:		
19	6a	(a) Inside the network		
20	6b	(b) Outside the network		
21	7	Does the system notify management of intrusions in real time?		
22	8	Are documented escalation procedures in place based on the threat-level?		
23	9	Does the system have intrusion prevention capabilities?		
24	10	Is the system configuration current and up-to-date?		
25	11	Is the system configured within manufacturer's specifications?		
26	12	Are all platforms being monitored (e.g. NT, Unix, Novell) as appropriate?		
27	13	Is access to the console controlled?		
28	14	Does the system monitor changes in critical system files?		
29	15	Can the system monitor changes in the Registry?		
30	16	Does the system monitor administrator activity?		
31	17	Is a qualified individual responsible for the regular monitoring of network traffic for potential intrusions?		
32	18	Does the system generate reports and immediately notify administrators of potential intrusions?		
33	19	Are there automated notification processes in place for detected intrusions?		
34		Section Rating:		
35		**Section C: Logging**		
36	20	Are unauthorized attempts to access information resources logged and included in a security violation report?		
37	21	Are intrusion detection logs and reports regularly reviewed and any necessary action taken?		

	A	B	D	F
5		**IT - IDS / IPS**		
6		**Objective: To evaluate whether the credit union is adequately securing its network environment with an Intrusion Detection System and/or Intrusion Prevention System to detect potentially harmful network activity.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
38	22	Are intrusion detection logs archived?		
39		Section Rating:		
40		**Section D: Change Management/Signature Updates**		
41	23	Are policy changes deployed manually?		
42	23a	a) If so, are policy changes consistent at all sensors?		
43	23b	b) If automatic, can the IDS determine which policy level is running at all sensors?		
44	24	Does the IDS system maintain an adequate list of attack signatures?		
45	25	Can signature updates be scheduled and fully automated?		
46	26	Are they up to date with the vendor releases?		
47	27	Have the updates been applied?		
48	28	Can custom signatures be added?		
49	29	Are custom signatures approved by management prior to implementation?		
50	30	Is documentation retained for the approval and change process?		
51	31	Are they verified by an independent party and is documentation retained of the verification?		
52	32	Is staff trained to add custom signatures?		
53		Section Rating:		
54		**Section E: Testing**		
55	33	Has an attack and penetration test ever been performed by credit union staff (such as the internal auditor)?		
56	34	Has an attack and penetration test ever been performed by an external party?		
57	35	Are penetration tests conducted on a regularly scheduled basis as well as whenever significant changes have occurred within the credit union network?		
58	36	Are the groups or individuals performing these tests appropriately bonded?		
59		Section Rating:		
60		**Overall Questionnaire Comments:**		
61				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B8
Comment: Detects unusual network activity, including attempts to break into the network; acts as a security camera for the network. This service may be outsourced.

Cell: B10
Comment: There are two types of intrusion detection systems: network-based and host-based. A network-based solution is similar to a firewall in that it acts as a traffic monitor on the network lines to monitor events. These types of detection systems would report denial of service attacks, scans and probes, as well as other suspicious events that a Firewall would not detect. Host-based solutions entail having software on every component. These components report back to a central controller if any abnormalities are detected. The host-based solution works well for reporting password attacks, attempts to obtain privileges or inject malicious code (like the antivirus software), vandalism, data theft, fraud, audit trail tampering, and security administration attacks.

Cell: D13
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B15
Comment: Network-based IDS monitors packets across the network while host-based IDS monitors packets on an individual server or PC.

Cell: B18
Comment: The CU should be able to explain its rationale for placement. If the IDS is in front of the firewall, it will catch problems earlier but is likely to identify more false positives. If the IDS is placed behind the firewall, it will identify problems later but is likely to generate less false positives.

Cell: B21
Comment: Does the system immediately inform management via e-mail, page, etc. if an attack is occurring?

Cell: B23
Comment: i.e., Will the IDS automatically attempt to stop an attack in real-time? Often called "intrusion prevention systems" (IPS), this is becoming an industry standard.

Cell: B24

Comment: Many times this is on a CD or on-line.

There should be a minimum configuration and placement as required by the vendor (this will probably not be so for Open Source systems).

Cell: B25
Comment: The manufacturer should specify a minimum machine configuration and placement of the sensor.

Cell: B26
Comment: Most corporate networks runs on Windows, but there are a variety of UNIX, Novell and AS400 environments that need to be monitored.

Cell: B27
Comment: Essentially, it is important that access is limited to critical personnel, so that the system cannot arbitrarily modified).

Cell: B28
Comment: Identify which system files are watched in the comments.

Cell: B29
Comment: The Registry in Windows 95/98/NT/2000 is a database that holds configuration data about the hardware and environment of the PC it has been installed in. It is made up of the SYSTEM.DAT and USER.DAT files. Many settings that were previously stored in WIN.INI and SYSTEM.INI in Windows 3.1 are in the Registry.

Cell: B30
Comment: Determine what administrative events are being monitored.

Cell: B33
Comment: Automatic notification processes include sending e-mails to designated administrators, paging administrators, security officers, assigned staff, etc.

Cell: D34
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B37
Comment: The management reporting function should provide adequate summaries of system activity, alerts and actions taken.

Cell: D39
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B41
Comment: If there are several sensors – then some automated deployment should be used.

Cell: D53
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B55

Comment: Attack and penetration testing, also known as "ethical hacking", is performed to find potential problems in the credit union's network and help implement procedures to close existing holes as well as minimize vulnerability to future problems. Ideally, these types of tests should include a thorough risk analysis of the Internet connection, define a security architecture adapted to the credit union's needs that takes into account the current architecture, assist the credit union in selecting components for the security structure, and identify opportunities to create, modify, or follow through with a sound security policy. These tests can be performed by either credit union staff or an external party.

Cell: D59
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - MEMBER ONLINE SERVICES**		
6		**Objective: To determine that adequate controls have been put into place to meet regulatory requirements for membership information safety and soundness and to meet all disclosure regulations.**		
7		**Question**	**Yes/No/ NA/ NR**	**Comments**
8		**Section A: Third Party Vendor Hosted Internet Banking**		
9	1	Is the internet banking application hosted by a third party? If no, go to Section B.		
10	2	Was the internet banking contract reviewed by legal counsel?		
11	3	Did the credit union secure a SAS 70 Report and/or other third party security review initially and annually thereafter to complete the due diligence requirements?		
12	4	Has the credit union addressed security on the connection between the credit union and the internet banking vendor?		
13		Section Rating:		
14		**Section B: CU Hosted Internet Banking**		
15	5	Does the credit union host the internet banking software internally? If no, skip this section.		
16	6	Is the software hosted on a server in a Demilitarized Zone (DMZ)?		
17	7	Are there design controls in place which construct and test changes to the software in a test setting?		
18	8	Have unnecessary services on the web server been disabled and appropriate controls implemented?		
19	9	Does the credit union obtain penetration tests and regular security scans of the Internet Banking network?		
20		Section Rating:		
21		**Section C: Internet Banking Controls**		
22	10	Do members have to submit a request to be enrolled?		
23	11	Do members receive an Internet Banking agreement which details their responsibilities and rights for using the system and all required consumer compliance disclosures?		
24	12	Do written procedures for Internet Banking User ID's and passwords include the following:		
25	12a	(a) Members change their password upon initial login?		
26	12b	(b) Minimum password requirements such as number of characters, type of characters, etc.?		
27	12c	(c) Maximum bad login attempts before locking out users?		
28	12d	(d) Procedures to reauthorize members who are locked out of their accounts?		
29	12e	(e) Reauthorized members change their password the first time they access their account again?		

	A	B	D	F
5		**IT - MEMBER ONLINE SERVICES**		
6		**Objective: To determine that adequate controls have been put into place to meet regulatory requirements for membership information safety and soundness and to meet all disclosure regulations.**		
7		**Question**	**Yes/No/ NA/ NR**	**Comments**
30	13	Are internet banking passwords maintained at the credit union?		
31	14	If yes to number 13, are passwords encrypted?		
32	15	If yes to number 13, is access to password files controlled?		
33	16	Can members change their address of record or other critical information via internet banking?		
34	17	Is there a process to verify critical information changed via internet banking was performed by the member?		
35	18	Does the software display a warning against unauthorized access to internet banking?		
36	19	Is administrative access limited to those employees who need access based upon their job description?		
37	20	Are administrative logs reviewed by a supervisor periodically?		
38	21	Are invalid logon attempts logged?		
39	22	Are inactive internet banking accounts monitored and controlled?		
40	23	Does the credit union have a written internet banking Procedure manual that provides guidance to employees?		
41	24	Are internet banking transactions processed in:		
42	24a	(a) Real-time?		
43	24b	(b) Batch?		
44	24c	(c) Other? (Please Describe).		
45	25	Are transactions reviewed and reconciled daily?		
46		Section Rating:		
47		**Section D: Bill Payer Controls**		
48	26	Does the credit union use a third party vendor to provide bill payment services to members? If no, skip this section.		
49	27	Was the bill pay contract reviewed by legal counsel?		
50	28	Did the credit union secure a SAS 70 Report and/or other third party security review initially and at least annually thereafter to complete the annual due diligence review?		
51	29	Do members have to submit a request to be enrolled?		
52	30	Do members receive a Bill Pay Agreement which details their responsibilities and rights for using the system and all required consumer compliance disclosures?		
53	31	Do members need to login to the bill pay software separately from the internet banking software?		
54	32	If yes, do written procedures for bill payer User IDs and passwords include the following:		
55	32a	(a) Members change their password upon initial login?		
56	32b	(b) Minimum password requirements such as number of characters, type of characters, etc.?		

	A	B	D	F
5		**IT - MEMBER ONLINE SERVICES**		
6		**Objective: To determine that adequate controls have been put into place to meet regulatory requirements for membership information safety and soundness and to meet all disclosure regulations.**		
7		**Question**	**Yes/No/ NA/ NR**	**Comments**
57	32c	(c) Maximum bad login attempts before locking out users?		
58	32d	(d) Procedures to reauthorize members who are locked out of their accounts?		
59	32e	(e) Reauthorized members change their password the first time they access their account again?		
60	33	Does the credit union have a written Bill Pay Procedure Manual that provides guidance to employees?		
61	34	Are bill pay transactions reviewed and reconciled daily?		
62		Section Rating:		
63		**Section E: E-Statements**		
64	35	Does the credit union offer E-Statements? If no skip this section.		
65	36	Does the credit union outsource the e-statement service?		
66	37	Was the vendor contract reviewed by legal counsel in the due diligence process?		
67	38	Is the credit union required to obtain and provide periodic SAS 70 and/or other independent controls review?		
68	39	Are members notified by e-mail that e-statements are available for review?		
69	40	Do members have to submit a request to be enrolled?		
70	41	Do members receive an agreement which details their responsibilities and rights for using the system and all required consumer compliance disclosures?		
71		Section Rating:		
72		**Section F: Account Aggregation Controls**		
73	42	Does the credit union offer account aggregation services to members? If no, skip this section.		
74	43	Is the account aggregation service provided by a third party vendor?		
75	44	Did the credit union complete a survey or other means to support the business case (justification) for offering account aggregation services?		
79	45	Is there a contract in place with the account aggregation providers which addresses:		
80	45a	(a) Liability of the credit union and provider?		
81	45b	(b) Statement processor will remain in compliance with legal and regulatory requirements?		
82	45c	(c) Document the authentication and verification process		
83	46	Did the credit union have legal counsel review the contract?		
84	47	Did the credit union secure a SAS 70 Report and/or other third party security review initially and at least annually thereafter to complete the annual due diligence review?		

	A	B	D	F
5		**IT - MEMBER ONLINE SERVICES**		
6		**Objective: To determine that adequate controls have been put into place to meet regulatory requirements for membership information safety and soundness and to meet all disclosure regulations.**		
7		**Question**	**Yes/No/ NA/ NR**	**Comments**
85	48	Do members have to submit a request to be enrolled?		
86	49	Do members receive an account aggregation agreement which details their responsibilities and rights for using the service and all required consumer compliance disclosures?		
87		Section Rating:		
88		**Overall Questionnaire Comments:**		
89				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B10
Comment: Appropriate legal counsel should review contracts prior to signing.

Cell: B11
Comment: Other Security Reviews can be penetration tests, security scans, etc.

Cell: B12
Comment: Private frame relays, Virtual Private Network, proper firewall configurations, encryption, etc.

Cell: D13
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B16
Comment: (Demilitarized Zone) A barrier between the Internet and a company's network. It is a subnet that contains a firewall and proxy server, which can be in separate servers or in one server. By putting web servers and email servers in the DMZ reduces the threats entering the network were sensitive data resides.

Cell: B17
Comment: The Network Questionnaire contains additional questions to evaluate the design and testing process.

Cell: B18
Comment: Disabling unnecessary services limits the vulnerability on that server.
Appropriate controls should include log monitoring, access, and change authority.

Cell: D20

Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B34
Comment: One best practice is to send a letter to the member's previous address of record verifying the change.

Cell: D46
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B49
Comment: Appropriate legal counsel should review contracts prior to signing.

Cell: B50
Comment: Other Security Reviews can be penetration tests, security scans, etc.

Cell: D62
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B68
Comment: Members could receive and e-mail notice, text message, or other form of notification. Whichever form is used, the notice should not divulge private information such as account numbers, etc...

Cell: D71
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B73
Comment: Account aggregation is a system by which individuals with internet-accessible accounts at several separate financial institutions can view all their balances and access their accounts from a single independent web page, using one set of confidential access codes.

Cell: B82
Comment: This is particularly important since aggregators typically offer their customers the equivalent of a single sign-on for many websites.

Cell: B83
Comment: Appropriate legal counsel should review contracts prior to signing.

Cell: B84
Comment: Other Security Reviews can be penetration tests, security scans, etc.

Cell: D87
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - Networks**		
6		**Objective: To determine whether management has identified and assigned the proper resources and accountability associated with Network Infrastructure**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8		**Section A: General**		
9	1	Does the credit union have a formal written policy or methodology to guide how networked applications are approved, prioritized, acquired, developed, and maintained?		
10	2	When new programs or services are under consideration, are they approved by the following prior to implementation:		
11	2a	(a) the board of directors		
12	2b	(b) the security officer		
13	2c	(c) the IT department		
14	3	Is there a schedule for equipment maintenance or replacement?		
15	4	Is any equipment maintained by an outside vendor? If yes, consider completing Vendor Oversight Questionnaire.		
16	5	Are there policies and procedures in place to ensure adequate management reporting or problems and resolution?		
17		Section Rating:		
18		**Section B: Network Access Controls/Account Policies**		
19	6	Are there written network password policies?		
20	7	Is there an expiration period for system passwords?		
21	8	Is there a minimum time set to allow password changes?		
22	9	Are account lockout options enabled?		
23	10	Are user accounts disabled for employees who have left the organization or change job responsibilities?		
24	11	Are inactive accounts removed from each group?		
25	12	Are guest accounts permitted?		
26	13	Has the administrator account been renamed to a strong user name?		
27	14	Have adequate steps been taken to ensure that the administrator account is protected?		
28	15	Do contingency measures exist to provide management access in the event the system administrator is not available?		
29		Section Rating:		
30		**Section C: Network Architecture/Design**		
31	16	Has management identified and reviewed network infrastructure access points and associated risks and vulnerabilities?		
32	17	Is a detailed listing of critical computer equipment and programs maintained?		

	A	B	D	F
5		**IT - Networks**		
6		**Objective: To determine whether management has identified and assigned the proper resources and accountability associated with Network Infrastructure**		
7		**Question**	**Yes/No/ NA/**	**Comments**
33	18	Does the credit union have a detailed network topology describing the connection points, services, hardware components, operating systems, addressing schemes, location of security devices, etc.		
34	19	Are policies, procedures, and practices in place describing how the network components (such as network servers, web servers, transaction servers, application and content servers, and electronic mail servers) are configured to ensure adequate security?		
35	20	Are the network services segregated to ensure data integrity and security (for example, web services and e-mail services should not be on the same server)?		
36	21	For each network component, does the credit union maintain a current inventory of the components' specifications (such as type of server, the operating system, required software, software version, and the last updates installed)?		
37	22	Does the credit union have written configuration policies and configuration checklists for servers, PCs, firewalls, routers, etc.		
38	23	Do the configuration policies and procedures address enabling and monitoring error logs and system auditing functions?		
39	24	Do the configuration policies and procedures address configuring components based upon the security required for the applications installed?		
40	25	Do the configuration policies and procedures address removing or disabling unnecessary network and operating system services?		
41	26	Do the configuration policies and procedures address implementing the necessary logical access controls?		
42	27	Do the configuration policies and procedures address replacing components when necessary?		
43		Section Rating:		
44		**Section D: Patch/Change Management**		
45	28	Does the credit union have written change management procedures that address management approval, scheduled upgrades, testing, and implementation?		
46	29	Does the change control documentation provide adequate audit trails, logs and support for all types of software modifications?		
47	30	Are there policies and procedures in place to handle emergency and temporary software fixes as well as new releases or upgrades?		
48	31	Are policies, procedures, and practices in place to allow the credit union to restore its previous configuration in the event a software modification adversely affects one or more systems?		

	A	B	D	F
5		**IT - Networks**		
6		**Objective: To determine whether management has identified and assigned the proper resources and accountability associated with Network Infrastructure**		
7		**Question**	**Yes/No/ NA/**	**Comments**
49	32	Are policies, procedures, and practices in place to maintain compatibility throughout the credit union's system environment?		
50	33	Is there a specific test environment set up, separate from the production environment to allow for testing installed patches and updates without destroying or damaging critical data?		
51		Section Rating:		
52		**Section E: Software Development**		
53	34	Are any of the credit union's applications developed in-house? If no, skip to Section F.		
54	35	Does management use a formal methodology or process to guide the acquisition, development, or maintenance of new or modified software?		
55	36	Are all affected parties involved in the development of systems specifications and business requirements?		
56	37	Is the Information Security Officer or Group a core member of all development projects?		
57	38	Are the application developers involved during the initial design and throughout the SDLC process?		
58	39	Are there policies, procedures, and practices in place that address unit, system, integration, and acceptance testing for all new or modified systems?		
59	40	Does the credit union maintain separate development, test, and production environments?		
60	41	Does management employ adequate version control techniques?		
61		Section Rating:		
62		**Section F: Network Monitoring**		
63	42	Do the credit union's policies and procedures establish network infrastructure performance standards for the following areas:		
64	42a	(a) Target throughput parameters?		
65	42b	(b) Hardware monitoring procedures?		
66	42c	(c) Transaction volume, response times, and bandwidth availability vs. bandwidth capacity?		
67	42d	(d) System uptime?		
68	43	Does management use automated network system monitoring tools?		
69		Section Rating:		
70		**Overall Questionnaire Comments:**		
71				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B9
Comment: Management should follow a series of predetermined and agreed upon steps for deploying applications. These steps should address, but may not be limited to, requirements analysis, vendor selection, project sponsorship and project management, approval processes, testing, user involvement and acceptance, and pre- and post-implementation reviews. Some of these steps may be optional and others required, depending on the magnitude and complexity of the project. If the application is developed by outside consultants or vendors, credit union management should be aware of (and approve of) the methodology employed by the third party developer or implementer.

Cell: B10
Comment: The Board, as well as all affected areas of the credit union, should be involved in any of the credit union's strategic initiatives relative to its Network Infrastructure at a high level. The Board's responsibility for the oversight and accountability for IS&T related services can not be delegated, and Board members should plan, approve and provide oversight for the entire Technology operations area. However, key senior management (from the business, technology, and security areas) must execute the Board's plan and keep the Board informed of key matters.

Cell: D17
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B20
Comment: The best practice is to set password to expire every 90 days for general staff and more frequently (e.g. 30 days or less) for administrators.

Cell: B22
Comment: A best practice for account lockouts is after three invalid attempts.

Cell: B25
Comment: The best practice is to periodically review and eliminate guest accounts. There should be justification for maintaining guest accounts.

Cell: D29
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B34
Comment: Sample policies, procedures, and practices include: Concept of least privileges for users to limit access; access to only a limited portion of the file system (e.g., document or CGI directories); access control lists configured to restrict administrative access and prevent unauthorized parties; and the automatic directory index disabled so directory browsing is prevented.

Cell: B35
Comment: It is a best practice to separate the back-office applications and data from the web servers and other components of the network (i.e. email server). If the web server (which is more vulnerable than any other part of the credit union's network) is compromised, member data or other sensitive information residing on the internal network will be protected if the systems are segregated.

Cell: B36
Comment: This is necessary to keep track of all hardware/software and to ensure compatibility of components and to assess vulnerabilities.

Cell: B41
Comment: Many network components have default passwords (well-known to hackers) . Network component configuration policies should require default passwords be changed prior to implementation of a new component on the network. Network password policies should be based on a thorough risk assessment (including classification of the sensitivity of data residing/accessible on the network).

Cell: D43
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B47
Comment: Emergency fixes are necessary due to the severity of problems being addressed. These types of changes should be infrequent.

Cell: B48
Comment: Network, operating system or application software modifications, if done improperly, can potentially have an adverse affect on one or more systems. Management's routine back-up and recovery procedures should provide the necessary assurance that the credit union will be able to restore to its previous configuration should operational problems occur. Management should practice restoring its systems on a routine basis so that they can be assured that procedures are sufficient should an actual emergency occur.

Cell: B49
Comment: It is imperative that the credit union's network, operating systems, and application systems are compatible. Various versions of these components may be incompatible resulting in operational problems, including slow response times, inaccurate or failed processing, etc. Management should have procedures in place to ensure the compatibility of these components. These procedures are generally centered around system and integration testing procedures, which involve testing numerous transactions from initial input to final output (including interface and reconciliation controls), as well as stress testing the system.

Cell: D51
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B57
Comment: SDLC - Software Development Life Cycle.

Cell: B58
Comment: Unit Testing: Testing which focuses on one particular program or module of a program.

System Testing: Testing an entire system or all the modules of a particular system.

Integration Testing: Testing which involves checking several units (programs or modules) together to make sure that they function together as intended. Interfaces (or bridges) between programs or modules within the system should be tested as part of the integration testing to assure that they continue to share and interpret information correctly.

Acceptance Testing: Testing which involves the end users certifying the product or systems functions as designed and meets end user requirements.

Cell: B59
Comment: Separate environments are desirable to avoid migrating bugs, problems, or errors to the production (live) environment. There may be occasion where this is not feasible due to the costs of obtaining and maintaining separate hardware and software components.

Cell: D61
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B63
Comment: Whether maintained by the credit union itself, or by a third party, website monitoring is critical to the success of a credit union's Internet service offerings. Effective monitoring involves more than just the router and web server. The credit union should also be looking at the number of requests that are coming "TO" the website, including those that are rejected. Rejected transactions, for whatever reason, result in a denial of service. Management needs to be aware of the number of times an authenticated user request is denied as well as the number of times an authorized user attempts to access its site. Some or most members will certainly be turned off if they attempt to initiate a transaction and their request is denied for no apparent reason. Similar to concurrent usage, management should also monitor when they have transaction peaks (e.g., first of the month, pay day) to ensure that its systems can handle the increased capacity. In addition, monitoring the types of transactions processed and the dollars associated with these transactions helps management with strategic planning. If a certain transaction type is not being requested, management may decide to discontinue the service. Alternatively, if a certain transaction type is very popular, management may decide to offer similar types of services in the future.

Cell: B64
Comment: Throughput refers to the maximum capacity that the system can handle successfully. If the system does not handle excess demand, transactions and data could be lost. When determining throughput, management needs to look at each e-Commerce system component individually as well as a whole (to avoid a potential bottleneck).

Cell: B68
Comment: Such as Simple Network Management Protocol (SNMP), HP Openview, or BMC Patrol.

Cell: D69
Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - Penetration Test Review**		
6		**Objective: To determine whether e-Commerce activities are subject to regular, independent review (internal and/or external) and whether management is appropriately addressing significant matters resulting from such reviews.**		
7		**Question**	**Yes/No / NA/**	**Comments**
8		**Section A: Penetration Test Agreement**		
9	1	Does the Penetration Test Agreement indicate that all compromised systems, if applicable, are restored to their initial configurations, if possible, and all files, tools, and other data left behind by the exercise is removed to the greatest extent possible?		
10	2	Did the firm engaged to perform the penetration test present management with a written report documenting the results of the test?		
11	3	Does the Penetration Test Agreement include client support to assist with any identified issues, mitigation strategies or vulnerability elimination steps contained in the report?		
12		Section Rating:		
13		**Section B: Penetration Test Report**		
14	4	Does the Penetration Testing Firm provide:		
15	4a	An Executive Summary Report		
16	4b	Technical Manager's Report		
17	4c	Technical Details Report		
18	5	Did management take timely action to address the weaknesses identified in the report?		
19		Section Rating:		
20		**Section C: Penetration Test Areas**		
21	6	What type of penetration test did the credit union contract for:		
22	6a	Blue Team Test		
23	6b	Red Team Test		
24	6c	Did the Penetration Test Scope include the following:		
25	6d	Policy Review		
26	6e	External Testing		
27	6f	Internal Testing		
28	6g	Social Engineering		
29	6h	Documentation and Reporting		
30	7	Did the Penetration Test Work Plan review these Network Security areas:		
31	7a	Network Surveying		
32	7b	Port Scanning		
33	7c	System Identification		
34	7d	Services Identification		
35	7e	Vulnerability Research & Verification		

	A	B	D	F
5		**IT - Penetration Test Review**		
6		**Objective: To determine whether e-Commerce activities are subject to regular, independent review (internal and/or external) and whether management is appropriately addressing significant matters resulting from such reviews.**		
7		**Question**	**Yes/No / NA/**	**Comments**
36	7f	Application Testing & Code Review		
37	7g	Router Testing		
38	7h	Firewall Testing		
39	7i	Intrusion Detection System Testing		
40	7j	Trusted Systems Testing		
41	7k	Password Cracking		
42	7l	Denial of Service Testing		
43	8	Did the Penetration Test Work Plan review these Wireless Security areas:		
44	8a	Wireless Networks Testing		
45	8b	Infrared Systems Testing		
46	8c	Communications Security		
47	8d	Voicemail Testing		
48	8e	Modem Testing		
49	9	Did the Penetration Test Work Plan review these Physical Security areas:		
50	9a	Access Controls Testing		
51	9b	Perimeter Review		
52	9c	Monitoring Review		
53	9d	Alarm Response Testing		
54	9e	Location Review		
55	9f	Environment Review		
56		Section Rating:		
57		**Overall Questionnaire Comments:**		
58				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: D12
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B15
Comment: Designed to go to senior management and the board (or appropriate subcommittee), the executive summary should not be overly technical.

Cell: B16
Comment: This report is designed to give a technically proficient audience a quick reference that discusses the work plan, findings, root causes of any issue, and overview of the path to mitigation.

Cell: B17
Comment: This report should have two goals: To give a technical reader an overview of the work and it's accomplishments; and Give a point and click path to mitigation.

Cell: D19
Comment: If you choose to comment on this rating, please use the cell to the right.

Cell: B22
Comment: Test when a client has full knowledge of the test, and the entire network is examined.

Cell: B23
Comment: A test exercise where the client staff may or may not know about the test, and the Penetration Team only seeks specific goals and targets.

Cell: B26
Comment: Examples of External Testing are External Network Vulnerability Assessment; External Network Penetration Testing, including malware and client attacks; Web Application Testing; and Dial up/VPN/RAS.

Cell: B27

Comment: Example of Internal Tests are Internal Vulnerability Assessment; Internal Network Penetration Test; Device Ruleset Review; Wireless Network Assessment.

Cell: B28

Comment: Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A social engineer runs what used to be called a "con game". For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural helpfulness of people as well as on their weaknesses. Appeal to vanity, appeal to authority, and old-fashioned eavesdropping are typical social engineering techniques.

Cell: B29

Comment: Examples of documentation are Compilation of Services, Risk Expression Report, Risk Mitigation Report, Delivery of Draft Report; Final Report, and Meeting of Results with staff.

Cell: B44

Comment:

All documents that are discovered during testing are submitted to analysis to identify potential information leaks, personal information or "hidden" document artifacts such as tracked changes. Other documents which are in the public domain are also examined, such as postings to bulletin boards, job advertisements, newsgroups etc.

Cell: B51

Comment: The advent of VoIP in combination with cordless phones provides the potential for a security event. A system could be compromised by a hacker tapping into the cordless signal (Radio Frequency Interference). A large number of breaches occur through PBX systems and this in combination with VoIP and cordless technology could result in a security event.

Cell: D56

Comment: If you choose to comment on this rating, please use the cell to the right.

	A	B	C
3		**IT - Policy Checklist**	
4		**Objective: Provide a general list of subjects normally covered in effective IT policies to assist in the examiner's review and evaluation of credit union IT policies.**	
5		**Section A: General IT Policies**	
6	1	Information security program (risk assessments, tests of controls, training, board reports)	
7	2	Designated security officer responsible for ensuring compliance (Appendix A, RR 748)	
8	3	Physical access controls and environmental controls for the data center	
9	4	System, network, e-mail, and database administration	
10	5	Firewall, router, and server security management	
11	6	Monitoring and backup of firewall and intrusion detection logs	
12	7	Wireless communication	
13	8	System access levels and administrative authorities granted by duty position	
14	9	Password administration for critical systems (network & EDP system logon, home banking)	
15	10	Use of encryption to protect sensitive data	
16	11	Use of modems (these can undermine firewall protection if not properly managed)	
17	12	Remote access for vendors and employees, if applicable	
18	13	Frequency of system patches and updates, logs maintained	
19	14	Virus protection and updates	
20	15	Vulnerability scanning and penetration tests	
21	16	Regulatory compliance of website content, e-forms, e-statements, applications, etc.	
22	17	Vendor management (Procurement, Contract Reviews, Service Level Agreements, Due Diligence Reviews, Vulnerability Scans, SAS 70s, Business Continuity Tests, etc.)	
23	18	Problem resolution and member service	
24	19	Backup & recovery procedures	
25	20	Testing of business continuity and disaster recovery plans	
26	21	Procedures for disposal of hardware, software, and documents containing sensitive information	
27		**Section B: Personnel Policies**	
28	22	Acceptable usage of Internet and e-mail	
29	23	No expectation of privacy	
30	24	Installation of personal software	
31	25	Prohibited use of e-mail for sending private/confidential information	
32	26	Disciplinary actions to be taken for non-compliance	
33	27	Password protection	
34	28	Information systems security awareness	
35	29	Code of ethics/fraud policy	
36	30	Procedures for removal of systems access upon termination of employment	
37	31	Acknowledgement form(s) to be signed by employees annually	
38	32	Evidence of periodic monitoring of compliance	
39		**Section C: IT Security Incident Response Policy**	
40	33	Definition of a security incident	
41	35	Containment procedures (isolate, do not use compromised systems)	
42	36	Preservation of evidence (make 2 copies of the hard drive of the compromised system)	
43	37	Contact persons to notify (including FBI or local law enforcement)	
44	38	A formal reporting process (notifying senior management, filing suspicious activity reports)	

	A	B	D	F
2		**Average of Assigned Ratings:**		
3		Examiner Assigned Rating:		
4				
5		**IT - REMOTE ACCESS**		
6		**Objective: To determine whether appropriate Remote Access Technologies policies, procedures, and practices are in place.**		
7		**Question**	**Yes/No/ NA/**	**Comments**
8	1	Does the credit union allow remote access to its systems? If no, skip this questionnaire.		
9	2	Are there policies and procedures in place which describe the authorization, authentication, and monitoring of remote access users such as:		
10	2a	(a) employees		
11	2b	(b) members		
12	2c	(c) vendors		
13	3	Is any data communicated to other companies via unsecured modems?		
14	4	Are methods in place to ensure that modems are not susceptible to unauthorized access?		
15	5	Has management created remote access user profiles?		
16	6	Has remote access only been granted based upon job duties and/or business needs ?		
17	7	Is vendor access to the credit union's network for diagnostic and/or maintenance activities properly restricted, approved, and monitored?		
18	8	Are there users with dial-in authority?		
19	9	Is dial-in access restricted to appropriate personnel?		
20	10	Have dial-in time limits been established?		
21	11	Is remote access privilege not included in the Administrator group?		
22	12	Have call back options been enabled?		
23	13	Is remote access monitored?		
24	14	Are authentication procedures in place for remote access?		
25	15	Does management approve and review remote access permissions initially and at least annually thereafter?		
26	16	Does management employ the proper procedures to detect and deny unauthorized remote access?		
27		Section Rating:		
28		**Overall Questionnaire Comments:**		
29				

Cell: B2
Comment: Examiners retain full discretion to assign the final questionnaire rating. This is a calculated cell that does not accept data entry.

Cell: B3
Comment: Examiner can add optional comments about the overall rating at the bottom of the questionnaire.

Cell: D7
Comment: The only data entry in the yellow cells should be Yes, No, NA, or NR. NA=Not Applicable, NR=Not Reviewed.

NA (Not Applicable) means you considered or reviewed the question (i.e.. Discussed with credit union officials) and the question is not applicable given the services the credit union provides or the systems the credit union uses.

NR (Not Reviewed) means the question or area was not reviewed.

Please note some of your answers will turn red. This does not necessarily mean a "wrong" or "bad" answer, but rather indicates there may be a need to ask more questions, or make suggestions.

Cell: B8
Comment: Software, installed in both machines, that allows a user at a local computer to have control of a remote computer via modem. Both users run the remote computer and see the same screen. Remote control operation is used to take control of an unattended desktop personal computer from a remote location as well as to provide instruction and technical support to remote users.

Cell: B13
Comment: Unsecured modems on networks can bypass firewalls and can allow back door entries to unauthorized users. War dialers dial up telephone numbers to determine which lines are connected to modems and fax machines in order to gain unauthorized access.

Cell: B14
Comment: Limit and control the number of modems residing in the credit union.

Cell: B21
Comment: The users should only have privileges on systems and access to functions that are required to perform their job function and assigned tasks. Access privilege may include read-only, read/write, or create/modify. Even read-only access poses risk since employees can print or copy sensitive customer information for inappropriate use. System administrator and security administrator level access allow an individual to change access privileges to systems and information. Individuals with these roles and privileges should have minimal transactional authority. Independent employees should monitor the system and security administrator activity logs for unauthorized activity.

Cell: B22
Comment: An authentication technique that calls the sender back. After connection is made, the receiving side breaks the connection and calls the sender to ensure that the logon was made from the authorized computer. Callback prevents a stolen ID and password from being used on a different machine.

Cell: B23
Comment: The entire program should be monitored to ensure employees and users are following policies and procedures.

Cell: B24
Comment: Secure access must be strictly controlled.
This can be done through strong password practices, public/private keys with strong pass phrases, etc.

Cell: B26
Comment: Proper firewall configurations, Intrusion Detection systems, monitoring of logs, etc.

Cell: D27
Comment: If you choose to comment on this rating, please use the cell to the right.

Type "X" when complete [ ]
Average of Assigned Ratings: [ ]
Examiner Assigned Rating: [ ]

Return to IS&T Checklist

IT - ROUTERS

Objective: To evaluate whether management practices relative to Router operation are adequate.

	Question	Yes/No / NA/	Comments
	Are the routers maintained by a third party? If No, skip Section A.		
	Section A: Router Maintained by Third Party		
1	Does documentation (i.e. topology maps) exist to identify the routers existing on the credit union's network?		
2	Does documentation exist for the current firmware version installed on the routers?		
3	Is physical access to the routers controlled?		
4	Is access to the routers controlled through the use of passwords or other means?		
5	Is telnet used to maintain the router?		
6	If router is maintained remotely, are communication links secured?		
7	Is router configuration reviewed and/or retained by internal employees?		
8	Is the router configuration reviewed regularly?		
9	Are commented, offline copies of all router configurations maintained and consistent with the actual configuration running on the router(s)?		
10	Is router log activity monitored and retained?		
	Section Rating:		
	Section B: Credit Union Maintained Router		
11	Does documentation (i.e. topology maps) exist to identify the routers that exist on the credit unions network?		
12	Does documentation exist for the current firmware version installed on the routers?		
13	Is physical access to the routers controlled?		
14	Is the responsibility for managing the routers assigned to a specific person?		
15	Is access to the routers controlled through the use of passwords or other means?		
16	Has training been provided to individuals responsible for router support and maintenance?		
17	Is a telnet, SSH, or HTTPS protocol used to maintain the router?		
18	If so, is access granted only to specific workstations on the internal network side of the router?		
19	If router is maintained remotely, are communication links secured?		
20	Is router configuration reviewed and/or retained by authorized internal employees?		
21	Is the router configuration reviewed regularly?		
22	Are commented, offline copies of all router configurations maintained?		
23	If yes, are they the same as the actual configuration running on the routers?		
24	Have backup router configuration files been tested, and how often?		
25	Are there written backup test procedures?		

IT - ROUTERS

Objective: To evaluate whether management practices relative to Router operation are adequate.

	Question	Yes/No / NA/	Comments
26	Has password encryption been turned on? (service password encryption)		
27	Are router logging capabilities turned on and are errors and blocked packets logged to a syslog host?		
28	Does the router block syslog traffic from untrusted networks? (This applies primarily to CISCO routers)		
29	Has the service timestamps command been used to ensure the complete date and time are stamped onto entries in the routers buffer log?		
30	Is router log activity monitored?		
31	Are all unneeded services shut down on the router(s)?		
32	Has "no ip directed-broadcast" been set on all interfaces? (This applies primarily to CISCO routers)		
33	Have all unused interfaces been shutdown?		
34	Has SNMP trap authentication been turned off to prevent a remote SNMP system shutdown request?		
35	Do the router(s) prevent forwarding packets with no clear route (no ip classless)?		
36	If not needed, has proxy ARP been disabled on all interfaces?		
37	Unless the router absolutely needs to autoload its startup configuration from a TFTP host, has network auto loading been disabled?		
38	Have access list filters been implemented to permit only those protocols and services that network users really need, and to explicitly deny everything else?		
39	Is there an access list filters corporate wide policy?		
40	Are router access lists configured to comply with corporate policy?		
41	Do access-list definitions start with "no access-list nnn" to make sure they start clean?		
42	Are access list port messages logged properly?		
43	Are internal addresses allowed to enter the router only from the internal interfaces?		
44	Are illegal addresses blocked at outgoing interfaces?		
45	Are packets blocked coming from the outside (untrusted) network that are obviously fake or commonly used for attacks?		
46	Are incoming packets blocked that claim to have the same destination and source address?		
	Section Rating:		

Overall Questionnaire Comments:

Type "X" when complete	
Average of Assigned Ratings:	
Examiner Assigned Rating:	

Return to IS&T Checklist

IT - Security Program

Objective: To determine whether the credit union has implemented a security program that considers electronic security risks to ensure the adequate protection of credit union and member data at all times.

	Question	Yes/No/ NA/	Comments
	Section A: General		
1	Has management developed and implemented a comprehensive security policy and program which describe the standards and procedures used to protect IT assets and member data?		
2	Is the security policy and program regularly reviewed and updated based upon technological or operational changes in the environment?		
3	Does the credit union have PC, network, Internet, and e-mail usage polices for employees and officials that have the following characteristics:		
3a	(a) prohibit employees from communicating account-specific or other sensitive member information via e-mail?		
3b	(b) prohibit employees from installing unauthorized software or hardware onto PCs and servers?		
3c	(c) require employees and officials to read and sign a statement indicating they have read and understand the usage policies?		
4	Does the credit union have policies and procedures in place to address incidents and events?		
5	Have any of the credit union's IT systems been compromised? If yes:		
5a	a) did management take the appropriate corrective action?		
6	Are incident logs maintained and reviewed?		
7	Has the ability to administer information security and alter system security parameters been limited to appropriate personnel?		
8	Are all operating systems appropriately configured to protect critical and sensitive data (e.g., disabling unnecessary services and accounts)?		
9	Does management review transactions to ensure:		
9a	(a) authentication of the user?		
9b	(b) integrity of the data?		
9c	(c) confidentiality of transactions?		
10	Does management maintain a current inventory of all security analysis tools it currently uses?		
11	Are policies and procedures in place that describe how and when encryption should be used to protect transmitted and stored information?		
12	Is encryption methodology tailored to specifically protect data deemed as sensitive?		
13	Are password files stored in encrypted format on a server that's securely separated from Internet facing servers?		
14	During member sessions, is sensitive data encrypted when it is transmitted or received via the Internet and over the credit union's network?		
	Section Rating:		

IT - Security Program

Objective: To determine whether the credit union has implemented a security program that considers electronic security risks to ensure the adequate protection of credit union and member data at all times.

	Question	Yes/No/ NA/	Comments
	Section B: Physical Security		
15	Has management included physical security in the overall security policy?		
16	Are there policies and procedures in place describing how access to the workspaces, data center, and other sensitive areas is secured and controlled?		
17	Are the locations of assets (servers, telecommunications equipment, etc.) analyzed to ensure that security is appropriate based on the sensitivity of the information stored on the asset?		
18	Does the physical security policy address computing (PCs, printers, software) and non-computing (e.g., confidential papers) assets?		
19	Does the credit union use fire resistant storage cabinets, boxes, or safes for the storage of computing and non-computing assets?		
	Section Rating:		
	Section C: Security Awareness		
20	Is a security awareness program in place? If yes:		
20a	(a) Is the program promoted by an Information Security Officer/Group or similar individual?		
20b	(b) Are user security-related responsibilities regularly communicated to employees?		
20c	(c) Are employees notified that compliance with security policies and procedures is constantly monitored?		
20d	(d) Does the security awareness program address IT security?		
21	Are industry (CERT, Bugtraq, etc.) and vendor advisories routinely monitored and appropriate actions taken to protect the credit union's information assets and member data?		
	Section Rating:		
	Section D: Monitoring		
22	Has responsibility for monitoring compliance with the security policies, procedures, and practices been clearly defined?		
23	Have information security tools been activated to record and report security events (such as security violations) that are defined in the information security policies?		
24	Are security monitoring reports regularly generated and reviewed?		
25	Are necessary corrective and/or disciplinary actions taken when security events occur?		
	Section Rating:		
	Section E: System Auditing		
26	Are the appropriate system auditing and logging functions enabled to capture audit trails related to network components?		
27	Is there a specific group or individual responsible for the oversight of system audit review?		
28	Are system, security, and server logs reviewed on a regular basis to detect inappropriate activity?		
29	Does management take timely action to address inappropriate activity once detected?		

IT - Security Program

Objective: To determine whether the credit union has implemented a security program that considers electronic security risks to ensure the adequate protection of credit union and member data at all times.

	Question	Yes/No/ NA/	Comments
30	Is there a policy or procedure in place for notification in the event that inappropriate activity is detected?		
	Section Rating:		
	Overall Questionnaire Comments:		

Type "X" when complete	
Average of Assigned Ratings:	
Examiner Assigned Rating:	

Return to IS&T Checklist

IT - Servers

Objective: To evaluate whether the Server Environment has been designed to adequately support the Network Infrastructure within the Credit Union.

	Question	Yes/No/ NA/	Comments
	Section A: General		
1	Does the credit union have a network schematic to identify servers in operation?		
2	Are servers maintained by internal personnel? If not indicate who maintains the servers.		
3	Is there a list of the hardware, software, and operating systems for each server in service?		
4	Is the operating software current for each server?		
5	Can it be determined when the last patch was applied to the software?		
6	Is the responsibility for patch management assigned to a specific person? If so, who?		
7	Does documentation of patch management exist?		
8	Have the servers been hardened?		
9	Is there more than one service on a server? If so, is each service on a separate Network Interface Card?		
	Section Rating:		
	Section B: Administrative Controls		
10	Is there remote access to the server software?		
11	If yes, is remote access provided to only authorized internal personnel?		
12	Is there an approval/review process in place for changes to software/services operating on the server?		
13	Is there a policy documenting which employees have administrative privileges for each server?		
14	Does the software have logging ability? Is it turned on?		
15	Is there a policy on reviewing the logs and an assigned reviewer?		
16	Is there documentation maintained of log reviews?		
17	Are the logs maintained for a specific length of time?		
	Section Rating:		
	Section C: Server Security		
18	Are any of the servers in a DMZ?		
18a	a) If yes, does the network schematic identify the servers in the DMZ?		
18b	b) If yes, is there documentation for the services running on each server in the DMZ?		
19	Has the credit union had a vulnerability scan?		
19a	a) If yes, did the scan include all servers?		
20	Is there documentation on the vulnerability scans performed?		
21	Was any action taken, and documented, to address the vulnerabilities identified?		
22	Is antivirus software on each server, and is it updated on a regular basis?		
23	Are there procedures and documentation to verify the latest virus software patch applied?		

IT - Servers

Objective: To evaluate whether the Server Environment has been designed to adequately support the Network Infrastructure within the Credit Union.

	Question	Yes/No/ NA/	Comments
24	Are there procedures for backing up the operating system and software for each server?		
25	Have server backups been tested and does documentation of the tests exist?		
26	Has management developed resolutions to the identified problems?		
	Section Rating:		
	Overall Questionnaire Comments:		

Type "X" when complete	
Average of Assigned Ratings:	
Examiner Assigned Rating:	

Return to IS&T Checklist

IT - VENDOR OVERSIGHT

Objective: To determine if the credit union has developed and implemented an adequate vendor due diligence oversight program.

	Question	Yes/No/ NA/	Comments
	Section A: General		
1	Has the board of directors approved a Vendor Oversight Policy?		
2	For the main software provider, did the credit union contact references and user groups to evaluate the service provider's reputation and performance?		
3	Did the credit union determine if the third party vendor is using subcontractors (other third parties) to supplement the services provided to the credit union?		
4	Did the credit union determine if the third party vendor or their subcontractors are foreign subsidiaries of U.S. Companies or Foreign Companies?		
5	Did the credit union request and evaluate the service provider's financial condition initially and then annually, thereafter?		
6	Did the credit union obtain and review audit reports/ SAS 70 reviews, initially and annually thereafter?		
7	Has the credit union reviewed the Client Considerations (controls) contained in SAS 70 Reports?		
8	Has the credit union implemented the Client Considerations (controls) contained in SAS 70 Reports?		
9	Did the credit union obtain and review regulatory examination reports initially and annually thereafter?		
10	Did the credit union obtain adequate information detailing the security measures in place to protect the facility, member data, etc.?		
11	Did the credit union secure a high level schematic of the third party vendors system?		
12	Did the credit union determine if the third party vendor has appropriate insurance coverage and receive confirmation of the coverage?		
13	Does the credit union regularly review reports documenting the service provider's performance?		
14	Does the credit union participate in user groups?		
15	Did the credit union review the service provider's business resumption contingency plans to ensure that any services considered mission critical for the institution can be restored within an acceptable timeframe?		
	Section Rating:		
	Section B: Contract		
16	Does the contract specify confidentiality requirements for member information? (Gramm Leach Bliley Act)		
17	Does the contract document the ownership of data and processes by each party entering into the contract?		
18	Does the contract outline the responsibilities, duties, and liability of each party?		

IT - VENDOR OVERSIGHT

Objective: To determine if the credit union has developed and implemented an adequate vendor due diligence oversight program.

	Question	Yes/No/ NA/	Comments
19	Does the contract address software details such as source code agreements, escrowing software, etc?		
20	Do contracts identify the roles, responsibilities, and controls for exchange of information between external parties?		
21	Does the contract address minimum service levels for each service provided by the vendor?		
22	Does the contract identify the monthly, quarterly, and annual reports which will be provided to the credit union to evaluate the vendor's adherence to service levels identified in the contract?		
23	Does the contract address minimum security procedures to protect member and credit union information?		
24	Does the contract address encryption for sensitive data on backup tapes and storage facilities?		
25	Does the contract identify services to be performed by the service provider including duties such a software support and maintenance, training of employees, etc.?		
26	Does the contract outline the obligations of the credit union?		
27	Does the contract address parties rights in modifying existing services performed under contract?		
28	Does the contract provide guidelines for contract re-negotiation?		
29	Did the credit union submit the contract to legal counsel for review prior to signing the contract?		
	Section Rating:		

Overall Questionnaire Comments:

Type "X" when complete	
Average of Assigned Ratings:	
Examiner Assigned Rating:	

Return to IS&T Checklist

IT - VIRUS PROTECTION

Objective: To determine whether the credit union utilizes virus protection and whether policies, procedures, and practices ensure that it is maintained up-to-date.

	Question	Yes/No/ NA/	Comments
	Section A: Virus Protection		
1	Does the credit union have virus protection software? If no, skip to section B.		
2	Is the virus protection software on each critical server connected to the network?		
3	Is the virus protection software on each personal computer connected to the network?		
4	Are the virus protection pattern files updated on a regular basis?		
5	If updates to virus pattern files are performed manually, is there adequate documentation by responsible parties showing updates have been performed on all personal computers and servers?		
6	If updates to virus pattern files are performed manually, are responsible parties signing off on the documentation as updates are completed?		
7	Does the credit union use an automated process to update the virus software pattern file on a regular basis?		
8	Does the credit union periodically verify that the automated scheduler is performing the updates?		
9	Is the virus software and update application located on a server or other appliance in the credit union network?		
10	If the update application is located on a server or other appliance, is the updated pattern file pushed out to each personal computer in the network automatically?		
	Section Rating:		
	Section B: Spyware Protection		
11	Does the credit union have spyware protection software? If no, skip to Section C:		
12	Does the credit union have spyware protection software on the network?		
13	Does the credit union have spyware protection software on personal computers with remote access?		
14	Is the credit union updating the spyware protection software on a timely basis?		
	Section Rating:		
	Section C: Spam Filtering		
15	Does the credit union use spam filtering software to reduce the amount of unsolicited e-mails?		
16	Does the credit union have a computer usage policy to keep employees from opening e-mails from unknown sources?		
	Section Rating:		
	Section D: Pop-up Blockers		
17	Does the credit union use pop-up blockers to eliminate/reduce the amount of unsolicited pop-up advertisements on the internet?		

IT - VIRUS PROTECTION

Objective: To determine whether the credit union utilizes virus protection and whether policies, procedures, and practices ensure that it is maintained up-to-date.

	Question	Yes/No/ NA/	Comments
18	Does the credit union have a computer usage policy to keep employees from opening pop-up ads?		
19	Are employees appropriately reprimanded for violations of computer use policies?		
	Section Rating:		

Overall Questionnaire Comments:

Type "X" when complete	
Average of Assigned Ratings:	
Examiner Assigned Rating:	

Return to IS&T Checklist

IT - WEB SITE REVIEW

Objective: To determine that adequate controls have been put into place to meet regulatory requirements for membership information safety and soundness and to meet all disclosure regulations.

	Question	Yes/No/ NA/ NR	Comments
	Section A: General Website Management		
1	Is there a board approved written Website Operating Policy that contains the following:		
1a	(a) A General Mission Statement?		
1b	(b) A statement on the type of information which is permissible on the site?		
1c	(c) List approved Internet links for the web site?		
1d	(d) Website monitoring requirements and assign an employee to be responsible for monitoring the site?		
1e	(e) Website change procedures and required documentation to retain for approved changes?		
2	Has a compliance review of the website been completed by the internal compliance officer or a reputable third party compliance expert?		
	Section Rating:		
	Section B: Websites Hosted Externally		
3	Is the web site hosted by a third party? If no, skip this section.		
4	Was the contract with the host reviewed by legal counsel in the due diligence process?		
5	Did the credit union obtain and review a SAS 70 Report or other type of external review of the third party initially and then at least annually thereafter?		
	Section Rating:		
	Section C: Website Design and Control		
6	Does a vendor or third party have the ability to make changes to the website?		
7	Does the CU have the ability to make design and content changes to the website?		
8	Are website changes approved by the IT committee and is documentation retained showing approved changes?		
9	Do independent CU personnel verify the changes after they are made and retain documentation of the review?		
	Section Rating:		
	Section D: Website Applications		
10	Does the credit union accept applications via the website? If no, skip this section.		
11	Are there written security procedures for accepting membership applications electronically?		
12	Is security for applications provided by a third party?		
13	Has responsibility been assigned to credit union personnel for reviewing and acting on the applications?		
14	Has the response time for reviewing and responding to applications been tested by management?		
	Section Rating:		
	Overall Questionnaire Comments:		

IT - WEB SITE REVIEW

Objective: To determine that adequate controls have been put into place to meet regulatory requirements for membership information safety and soundness and to meet all disclosure regulations.

	Question	Yes/No/ NA/ NR	Comments

Type "X" when complete	
Average of Assigned Ratings:	
Examiner Assigned Rating:	

Return to IS&T Checklist

IT - Wireless Local Area Networks (WLANs)

Objective: To determine the adequacy of controls over wireless local area networks (WLANs) utilizing technology compliant with IEEE 802.11b ("Wi-Fi") and related wireless networking technology standards. Elements of this work program may also apply to wireless wide area networks (WWANs) utilizing this technology.

	Question	Yes/No/ NA/	Comment
	Section A: General		
1	Are WLAN/WWAN policies and procedures adequate?		
2	Does the risk assessment program address WLANs?		
3	Are WLAN equipment and security devices included in the topology for the CU Network Infrastructure?		
4	Have key employees received appropriate training regarding network, application, and security controls?		
5	Is there a trained backup to the primary WLAN administrator?		
6	Is there a current inventory of WLAN/WWAN Hardware Devices and Network Interface Cards (NICs)?		
7	Is there a copy of vendor documentation for the devices used by the CU?		
8	Is WLAN included in audit work plans to ensure compliance with policies and procedures?		
	Section Rating:		
	Section B: Security		
9	Have default security settings for WLAN access points (APs) and wireless routers/bridges been appropriately configured as follows:		
9a	(a) The default SSID changed?		
9b	(b) The broadcast feature disabled?		
9c	(c) Default admin user IDs and passwords changed using strong passwords?		
9d	(d) MAC address filtering enabled?		
9e	(e) SNMP disabled for wireless equipment?		
9f	(f) DHCP been disabled?		
9g	(g) Default network IP addresses changed?		
9h	(h) 128-bit WEP encryption enabled with dynamic keys?		
9i	(i) WEP keys changed from default settings?		
10	Are WEP keys changed frequently?		
11	Are WLANs turned off after business hours?		
12	Does the CU use end-to-end encryption based upon proven encryption technology?		
13	Does the CU utilize VPN with the WLAN?		
14	Does the CU utilize IPsec with the WLAN?		
15	Does the CU utilize any supporting technology to protect the data stream?		
16	Has a firewall been installed between the wired infrastructure and the WLAN/WWAN?		
17	Does the CU use an additional form of authentication (such as RADIUS or Cisco's LEAP) to improve the security of the client/AP authentication process?		
18	Do the procedures for client computers with wireless NICs include:		
18a	(a) Deploying personal firewalls?		
18b	(b) Deploying anti-virus software?		