	A	B	C	D	E	F
1	**Credit Union:**					
2	**Charter #:**					
3	**E-Commerce Questionnaire (EC-1)**					
4	**Sec. #**	**Que. #**	**Sub-Que. #**	**Question**	**Y/N/ NA/ NR**	**Comments**
5	**1**	**General**				
6	1	1	0	Does the credit union engage in E-Commerce activities with its members via the Internet, world-wide web, home banking, etc.		
7	1	2	0	Are E-Commerce products and services considered to be critical to the credit union's goals and strategies?		
8	1	3	0	Have adequate policies and procedures been developed for the credit union's E-Commerce activities?		
9	1	4	0	Does the credit union have an E-Commerce organization chart or listing of key E-Commerce staff?		
10	1	5	0	Has management established an E-Commerce oversight committee comprised of representatives from applicable departments such as Marketing, Compliance, Operations, Information Systems and Security?		
11	1	6	0	Does the credit union Board of Directors receive reports on E-Commerce activities on a regular basis?		
12	1	7	0	Does the credit union have an a) informational, b) interactive or c) transactional website?		
13	1	8	0	Is the website hosted by a) the credit union, b) vendor or c) third party?		
14	1	9	0	Is the website content developed and maintained by the credit union?		
15	1	10	0	Does the credit union offer the following services electronically:		
16	1	10	1	Member Application		
17	1	10	2	Share Account Application		
18	1	10	3	Share account transfers		
19	1	10	4	Loan Applications		
20	1	10	5	Loan payments		
21	1	10	6	Bill payment		
22	1	10	7	Account Balance Inquiry		
23	1	10	8	View Account History		
24	1	10	9	Download Account History		
25	1	10	10	Share Draft Orders		
26	1	10	11	Merchandise Purchase		
27	1	10	12	Electronic Cash		
28	1	10	13	Wire Transfers		
29	1	10	14	Other (describe)		
30	**2**	**Risk Assessment**				
31	2	1	0	Are there policies, procedures and practices in place for performing risk assessments to identify internal and external threats and vulnerabilities associated with E-Commerce?		
32	2	2	0	Do these policies and procedures address Operational/Transactional, Security, Reputation and Compliance Risks?		
33	2	3	0	Has a risk assessment been performed for the credit union's E-Commerce activities?		
34	2	4	0	Does management actively reevaluate risks associated with technological and operational changes in E-Commerce?		
35	2	5	0	Has management considered and is it continually monitoring the risks associated with outsourcing relationships?		
36	**3**	**Compliance and Legal**				
37	3	1	0	Is legal counsel consulted for significant matters such as E-Commerce contracts, partnerships and affiliations?		
38	3	2	0	Are changes to applicable laws and regulations actively monitored and are policies and procedures updated accordingly?		
39	3	3	0	Have appropriate procedures been put in place to ensure that E-Commerce transactions are legally binding (e.g., verifiably performed by the appropriate party) and cannot be repudiated?		
40	3	4	0	Has management determined whether E-Commerce activities are included in its bond coverage and, if so, has management determined if the coverage is sufficient?		
41	3	5	0	Does management review the credit union's bond coverage annually to ensure that it is adequate in relation to the potential risk?		
42	3	6	0	Has management considered the legal ramifications associated with providing E-Commerce services to multi-state and multinational members?		
43	**4**	**Audit and Consulting Services**				
44	4	1	0	Are E-Commerce activities subject to periodic internal (internal audit) and/or external (SAS 70 or financial statement) audits and quality reviews?		

	A	B	C	D	E	F
1	**Credit Union:**					
2	**Charter #:**					
3	**E-Commerce Questionnaire (EC-1)**					
4	**Sec. #**	**Que. #**	**Sub-Que. #**	**Question**	**Y/N/ NA/ NR**	**Comments**
45	4	2	0	Has management prioritized the issues disclosed in the most recent audit or quality review?		
46	4	3	0	Has management corrected, or is in the process of correcting, these issues?		
47	4	4	0	Has management performed and documented an assessment to determine if Attack and Penetration Testing should be used as a means of identifying, isolating and confirming possible flaws in network and security architecture?		
48	4	5	0	If the assessment warrants penetration testing, has management performed, contracted or planned to contract for these services?		
49	4	6	0	If a penetration test has been performed, has management addressed, or is in the process of addressing, identified vulnerabilities?		
50	**5**	**Vendor Management**				
51	5	1	0	Has management assessed long-term strategic and short-term tactical plans for current and future E-Commerce outsourcing activities?		
52	5	2	0	Does management actively monitor whether critical, outsourced service providers continually meet the credit union's E-Commerce needs (i.e. hardware, software, network services)?		
53	**6**	**Member Service and Support**				
54	6	1	0	Does management have a process in place to adequately track and resolve member support issues (e.g., member technical support, incident reports, and FAQ's)?		
55	6	2	0	Has management established and tailored member service level goals based on their business needs and unique field of membership expectations?		
56	**7**	**Personnel**				
57	7	1	0	Is the credit union adequately staffed and trained with respect to its E-Commerce strategy?		
58	7	2	0	Does an adequate segregation of duties exist between conflicting E-Commerce related responsibilities?		
59	7	3	0	Does the credit union have a process in place to handle the addition, modification or deletion of employee's access due to status changes, i.e. terminations, transfers, promotions?		
60	7	4	0	Has credit union management implemented practices to address the recruitment and retention of E-Commerce technical staff?		
61	**8**	**System Architecture and Controls**				
62	8	1	0	Are adequate network, system and application diagrams (i.e. topologies) maintained?		
63	8	2	0	Is an adequate inventory of E-Commerce hardware and software maintained?		
64	**9**	**Security Controls**				
65	9	1	0	Does the credit union have an adequate security program in place (i.e., documented policies and procedures) which covers protecting critical data and facilities?		
66	9	2	0	Does management monitor credit union staff activity to ensure compliance with established security policies and procedures?		
67	9	3	0	Have safeguards been implemented to mitigate the risk of confidential member and servicing information being disclosed to or modified by unauthorized users?		
68	9	4	0	Have authentication techniques/controls been put in place to block unwanted communications into and out of the credit union network (i.e., Firewall)?		
69	9	5	0	Have member session controls been put in place to ensure that access is only granted to the appropriate users?		
70	9	6	0	Have controls been put in place that automatically log-off a session (member or other users) as a result of inactivity?		
71	9	7	0	Has management classified data based upon its sensitivity, perceived value and the impact to management in the event of its loss?		
72	9	8	0	Have the various types of data communicated on the credit union's network been categorized according to its sensitivity?		
73	9	9	0	Has the credit union implemented adequate security policies and procedures according to the sensitivity and importance of data?		
74	9	10	0	Is a criteria in place which determines the level of encryption that shall be used for the varying degrees of sensitive information?		
75	9	11	0	Is an appropriate level of encryption being utilized to protect sensitive data (data residing on the webserver or transmitted during a session)?		
76	9	12	0	Are effective and thoroughly tested security tools used to monitor internal and external threats?		

	A	B	C	D	E	F
1	**Credit Union:**					
2	**Charter #:**					
3	**E-Commerce Questionnaire (EC-1)**					
4	**Sec. #**	**Que. #**	**Sub-Que. #**	**Question**	**Y/N/ NA/ NR**	**Comments**
77	9	13	0	Does the credit union ensure that virus identification and protection software is implemented, monitored and updated when required?		
78	9	14	0	Does the credit union have an intrusion detection system?		
79	9	15	0	If yes, is it a real-time intrusion detection system?		
80	9	16	0	Does the credit union respond to potential intrusions in a timely manner?		
81	**10**	**Business Continuity**				
82	10	1	0	Has disaster recovery relating to E-Commerce been incorporated into the credit union's overall business continuity plan?		
83	10	2	0	Does the credit union review its plan, at least annually, based on changes in technology, its infrastructure or E-Commerce activities?		
84	10	3	0	Is the plan tested on a regular basis and are the test results analyzed to identify necessary changes?		
85	10	4	0	Has the credit union developed incident response and escalation procedures for technical, security or member concerns?		
86	**11**	**Performance Monitoring**				
87	11	1	0	Has the credit union established and implemented adequate performance monitoring procedures for E-Commerce activities?		
88	11	2	0	Is the performance of E-Commerce activities monitored by management against long-term and short-term plans, or member demands?		

Cell: D8
Comment: Policies and procedures should be developed or updated to specifically address E-Commerce operations. These might include network and infrastructure architecture; vendor management; information security; application development and maintenance; computer operations; technical support; member support and service; backup and recovery; business continuity planning, etc.

Cell: D12
Comment: Informational: displays general information such as loan/share rates, credit union information, privacy notice, etc.
Interactive: members can request information such as share and loan balances, account statements, disclosure statements, etc.
Transactional: members can initiate or perform transactions such as paying bills, making loan payments, transferring money (between one or more credit union accounts; between the credit union and third parties), completing loan applications, completing member applications, opening new share accounts, etc.

Cell: D13
Comment: Vendor - e.g. primary loan/share processor which is now providing website services
Third Party - e.g. service organization used specifically for hosting the website, website content, bill paying services, etc.

Cell: D31
Comment: Internal threats: social engineering, terminated or disgruntled employees, vendors, viruses, chat programs, etc.
External threats: browsers, unsecured modems, hackers, crackers, other unauthorized users, etc.

Cell: D35
Comment: Management should periodically perform a risk assessment of activities performed by service organizations on the credit union's behalf. This assessment should address the service organization's financial stability, business practices, quality of service being rendered, remote access to the credit union's network by service organization personnel, etal.

Cell: D44
Comment: Service organizations are not required to obtain SAS 70 reports. Credit union management should perform a risk assessment and due diligence process to determine whether a SAS 70 report is desired for its vendor(s). If a report is obtained, Internal auditors or the SC should reassess and test user control considerations included in the report. Examiners should reevaluate management's due diligence and risk assessment processes. If a report is available, the examiner should evaluate management's response to issues raised in the report.

Cell: D47
Comment: Credit unions are not required to perform nor are they required to engage a third party to perform Attack and Penetration Tests.

Cell: D49
Comment: Attack and Penetration Test results are sensitive and confidential. Review engagement letter and executive summary of the report only, as well as the BOD or committee minutes. Obtain SE approval before reviewing detailed findings and observations included in the report. Determine whether Internal Audit or Supervisory Committee is providing necessary oversight for issues raised in the report.

Cell: D51
Comment: Considerations might include costs and benefits of maintaining necessary computing equipment in-house, service organization's computing capacity, service organization's ability to meet credit union's ongoing needs, security concerns, human resource requirements, etc.

Cell: D54
Comment: E-Commerce related member service and support issues should be responded to by properly trained individuals and tracked separately. Procedures should also ensure that recurring or significant service and support issues are given priority, and reported to management timely so that they can be researched and resolved.

Cell: D58
Comment: For example, a segregation of duties should exist between individuals making programming changes to website content and those responsible for placing changes into the production environment, and individuals responsible for Firewall configuration settings and those responsible for monitoring the Firewall, etc. If an appropriate segregation of duties does not exist (due to the technical nature of responsibilities, inadequate staffing, etc.), management should be aware of the potential conflict and require that a periodic internal or external review of these conflicting responsibilities be performed.

Cell: D62
Comment: Management should maintain up-to-date diagram(s) of the network, system and application components comprising its E-Commerce operations. The diagram(s) may vary in the level of detail, but at a minimum, should depict any internal or external connectivity and the means by which this connectivity occurs (i.e. modem, Internet). The diagram can be used to visualize how the E-Commerce operation works and to identify any vulnerability points.

Cell: D67
Comment: Safeguards might include encrypting member data as it is being transmitted via the Internet; storing member data on computers with restricted access; real time intrusion detection and prevention; etc.

Cell: D68
Comment: Controls might include configuring the Firewall to filter and disallow unwanted communications; requiring that users enter a unique password when accessing accounts over the Internet; denying access to users who do not enter a correct password within three tries; resetting users' passwords only after proper identification has been presented, etc.

Cell: D76
Comment: Security tools might include Firewalls, real time intrusion detection systems, and anti-virus software, as well as responding to security advisories, installing operating system updates and patches as they become available, etc.

Cell: D80
Comment: It is a best practice for the intrusion detection system to automatically alert (page) network administrators when potential intrusions occur. The detection system might also shut-off the port being intruded, capture critical information about the potential intruder, and disallow any further communication with the potential intruder until the contact has been researched.

Cell: D82
Comment: Management should continually balance members' reliance on Internet service offerings against its ability to provide uninterrupted services. The fact that members can use alternative delivery channels (i.e. coming into a branch, ATM, etc.) may not be a sufficient reason to exclude E-Commerce operations from disaster recovery planning efforts.

Cell: D87
Comment: Ideally, management should use an automated tool to monitor performance of all components relative to E-Commerce operations. Components might include the webserver or transaction server, Domain Name System (DNS) server, production LAN servers, etc. Performance metrics requiring monitoring might include average and peak processor utilization, average response time for various transaction types, network availability, etc. If website is hosted by a third party, management should ensure that the vendor provides this type of information for its review and consideration.

	A	B	C	D	E	F	G	H
1	**Credit Union:**							
2	**Charter #:**							
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
5	**1**	**General**						
6	1	0	0	1	0	Have information systems strategies, long term strategic, and short term tactical plans been formulated and approved by the Board of Directors to support the overall E-Commerce strategy and information systems requirements of the credit union?		
7	1	0	0	2	0	Does the credit union use a formal methodology/process to guide how E-Commerce applications are approved, prioritized, acquired, developed, and maintained?		
8	1	0	0	3	0	When new E-Commerce ideas or strategic initiatives are under consideration, are they reviewed by the following: - the business-side of the credit union, - the technology side of the credit union, and - the security side of the credit union?		
9	1	0	0	4	0	Are the appropriate responsibilities for maintaining the website spread amongst all applicable departments (e.g., Marketing, Information Technology, Information Security, Legal, Customer Service, and Fraud)?		
10	**2**	**Risk Assessment**						
11						Objective: To determine whether management has properly identified and addressed all the risks associated with E-Commerce.		
12	2	0	0	1	0	Do risk assessment policies and procedures address the following? - The conditions for when a risk assessment is to be performed - An up-to-date account of perceived threats - A standard for determining critical applications and data		
13	2	0	0	2	0	Does the risk assessment definition criteria detail whether a threat is: + an acceptable risk? + a risk to be monitored and managed? + a risk to be eliminated?		
14	2	0	0	3	0	Does the credit union maintain a current list of critical assets, applications and data that is: + categorized? + quantified? + prioritized?		
15	**3**	**Compliance and Legal**						
16						Objective: To evaluate whether management practices relative to E-Commerce have been designed to properly address regulatory compliance and other legal issues.		
17	3	0	0	1	0	Are procedures sufficient to ensure compliance with applicable laws and regulations such as Fair Credit Reporting Act (FCRA), Electronic Funds Transfer Act (EFTA), Truth In Savings Act (TISA), and Truth in Lending (TIL)?		
18	3	0	0	2	0	Has management implemented procedures to ensure that member transactions subject to the Bank Secrecy Act (i.e. individual/aggregate transactions totaling $10,000 or more) are flagged and reviewed for compliance and necessary reporting?		
19	3	0	0	3	0	When new E-Commerce relationships are established, are the service agreements and/or disclosures provided to members commensurate with E-Commerce services offered?		
20	3	0	0	4	0	Does management routinely monitor this process to ensure agreements and disclosures are updated and distributed as necessary?		
21	3	0	0	5	0	Is there a policy in place that adequately addresses the collection and use of personal information as it relates to member privacy?		
22	3	0	0	6	0	Are comprehensive privacy disclosures provided to all on-line users?		
23	3	0	0	7	0	Does the credit union monitor and enforce compliance with the privacy disclosures included on the website?		
24	3	0	0	8	0	Are there policies and procedures in place describing methods utilized to validate transactions, e-mails, and other contractual obligations relating to E-Commerce?		
25	3	0	0	9	0	Are warning banners in place to clearly state that unauthorized access or use is not permitted and may constitute a crime punishable by law?		
26	3	0	0	10	0	Do policies and procedures address the periodic review of contracts, partnerships, and affiliations by legal counsel?		
27	3	0	0	11	0	Does the credit union have multi-state or multi-national members using E-Commerce services?		

	A	B	C	D	E	F	G	H
1				Credit Union:				
2				Charter #:				
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
28	3	0	0	12	0	For multi-state/multi-national considerations, does legal counsel review the credit union's E-Commerce policies, procedures, and practices to ensure compliance with the regulations applicable to the states/countries in which members reside?		
29	3	0	0	13	0	Does the credit union proactively review the adequacy of its bond coverage as E-Commerce services are modified (new, revised or terminated services, etc.)?		
30	**4**	**Audit and Consulting Services**						
31						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.		
32	4	0	0	1	0	Does the independent review function provide for adequate oversight during all phases of the planning and implementation of the credit union's E-Commerce strategy and infrastructure?		
33	4	0	0	2	0	Did the independent review function address requirements analysis, vendor selection and due diligence, risk assessments, and alignment of E-Commerce strategies to the overall business strategy?		
34	4	0	0	3	0	Does the function include a review of inter-departmental responsibilities for those departments involved in E-Commerce activities?		
35	4	0	0	4	0	Does the annual audit plan include a review of E-Commerce products, services, and controls?		
36	4	0	0	4	0	Does it appear that the independent review function is adequately staffed?		
37	4	0	0	5	0	Does the function include an on-going review of E-Commerce products, services, and controls between scheduled audits to ensure that any significant changes are appropriately addressed?		
38	4	0	0	6	0	Are there policies and procedures in place which describe how and when E-Commerce-related independent reviews are performed? For example, they may include: - Security policy and procedure reviews - Attack and penetration testing - Regulatory compliance reviews - Member privacy reviews - Application development and maintenance reviews - Incident response and business continuity plan reviews - Virus detection and protection reviews		
39	**5**	**Vendor Management**						
40						Objective: To determine whether appropriate vendor management policies, procedures, and practices exist.		
41	5	1	**Vendors, Partners, and Affiliates**					
42	5	1	0	1	0	Are there procedures in place detailing acceptance criteria, approval of and on-going monitoring and management of outsourced vendors? For example are: - Requirements analyses performed to identify the credit union's needs? - Requests for Proposals (RFP's) developed and distributed? - Multiple bids obtained and reviewed from reputable vendors? - Vendor contracts reviewed by legal counsel? - Roles, responsibilities, and controls identified for the exchange of information between the credit union and any external parties? - Service level agreements in place detailing performance standards and criteria? - Service level agreements monitored for adherence?		
43	5	1	0	2	0	Do vendor contracts address minimum security procedures to protect member and credit union information?		
44	5	1	0	3	0	Does management periodically review security procedures employed by their vendors to ensure that minimum requirements are met?		
45	5	1	0	4	0	Are minimum standards established and are due diligent reviews performed (financial statement review and liability analysis) on potential business alliances prior to establishing a business relationship?		
46	5	1	0	5	0	Are there network and/or remote dialup connections between the credit union, its facilities, outside vendors and/or strategic partners? If so, what types of connections are used by business partners when accessing the internal network (dedicated modem, time-based access, modem call-back, SmartCards, etc.)?		

	A	B	C	D	E	F	G	H
1			Credit Union:					
2			Charter #:					
3	E-Commerce Review Program (EC-2)							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
47	5	1	0	6	0	Does documentation exist depicting the internal network and connections to external parties? For example, connections to: - Credit Bureaus - Credit Card Processors - Web Content Provider - Bill Pay Servicer - Automated Clearing House (ACH) - Internet Service Provider (ISP) - Other financial institutions		
48	5	2	**Internet Service Providers (ISP)**					
49	5	2	0	1	0	Does the credit union utilize one or more Internet Service Providers (ISP) to support access to its E-Commerce products and services? - Identify the ISP, or ISPs if redundancy is utilized - Describe the connectivity between the credit union's network and the ISP(s) - Identify which party has responsibility for each connectivity component (e.g., Routers, CSU/DSU)		
50	5	2	0	2	0	Is the credit union aware of, and working closely with the ISP to ensure that all security-related issues are identified, jointly addressed, and resolved?		
51	5	2	0	3	0	Does the ISP meet the credit union's minimum standards relevant to: - Network Security? - Network Performance? - Internet Availability?		
52	5	3	**Application Service Provider (ASP)**					
53	5	3	0	1	0	Does the credit union utilize an Application Service Provider (ASP) to develop and support its E-Commerce products and services? If not, skip this section.		
54	5	3	0	2	0	Is the credit union aware of, and working closely with the ASP to ensure that all security-related issues are identified, jointly addressed, and resolved?		
55	5	3	0	3	0	Does the ASP meet the credit union's minimum standards relevant to: - Application Security? - Session Management? - System Development Life Cycle methodologies?		
56	5	3	0	4	0	Does the service provider maintain production and development systems on separate networks?		
57	5	4	**Content Service Provider**					
58	5	4	0	1	0	Does the credit union utilize a Content Service Provider (CSP) to code, integrate, and install the various content for E-Commerce products and services? If not, skip this section.		
59	5	4	0	2	0	Is the credit union aware of, and working closely with the CSP to ensure that all security, privacy, and disclosure-related matters are identified, jointly addressed and resolved?		
60	5	4	0	3	0	Does the CSP meet the credit union's minimum standards relevant to: - Information security and confidentiality? - Content accuracy? - Usability? - Availability?		
61	**6**	**Member Service and Support**						
62						Objective: To evaluate whether management has implemented the necessary policies, procedures, and practices to ensure that member service and support issues are adequately responded to and resolved in a timely manner.		
63	6	0	0	1	0	Is there a separate member support department responsible for resolving member complaints or inquiries related to E-Commerce activity?		
64	6	0	0	2	0	Does the credit union utilize an automated call-tracking system for member complaints and inquiries?		
65	6	0	0	3	0	Does management routinely generate and monitor reports to ensure member service level goals are met and adjusted as needed?		
66	6	0	0	4	0	Does management proactively inform the membership of maintenance or other technical issues that may affect access to E-Commerce activities through detailed real time/on-line messages?		
67	6	0	0	5	0	Are member service levels considered with respect to E-Commerce growth projections and resource planning?		
68	**7**	**Personnel**						
69						Objective: To determine whether management has appropriately assessed and provided for the credit union's human resources needs.		
70	7	1	**Hiring, Training and Retention**					

	A	B	C	D	E	F	G	H
1	**Credit Union:**							
2	**Charter #:**							
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
71	7	1	0	1	0	Are the skills and experience required for key positions supporting E-Commerce activities clearly defined before hiring staff?		
72	7	1	0	2	0	Does management monitor and adjust staffing levels based on human resource needs?		
73	7	1	0	3	0	Are background checks routinely performed before hiring information technology professionals?		
74	7	1	0	4	0	Has management implemented any types of incentives for the recruitment and retention of staff responsible for E-Commerce activities?		
75	7	1	0	5	0	Is periodic technical training provided to employees to ensure skill levels are commensurate with job responsibilities and reflect emerging technologies?		
76	7	1	0	6	0	Is there a process in place to monitor compliance with training requirements?		
77	7	1	0	7	0	Are certain targeted positions supported by succession planning and cross-training?		
78	7	1	0	8	0	Are new hires made aware of the credit union's policies, procedures and standard practices as well as the disciplinary actions to be taken for non-compliance?		
79	7	1	0	9	0	Does management routinely monitor for compliance with stated policies, procedures, and standards?		
80	7	1	0	10	0	Are employees required to sign a policy compliance statement (e.g., Code of Ethics, Information Protection Statement) when hired by credit union?		
81	7	1	0	11	0	Does management routinely provide employees with performance appraisals based upon pre-determined performance criteria?		
82	7	2	**Business Functional Organizations**					
83	7	2	0	2	0	Does senior management continually provide the necessary direction and oversight for key decisions relevant to E-Commerce activities?		
84	7	2	0	3	0	Identify the key department(s) and individual(s) responsible for the planning, direction, creation, maintenance, and update of the E-Commerce products and services.		
85	7	2	0	4	0	Identify department(s) and key individual(s) responsible for content development.		
86	7	2	0	5	0	Identify department(s) and key individual(s) responsible for content testing.		
87	7	2	0	6	0	Identify department(s) and key individual(s) responsible for privacy policy and disclosure.		
88	7	2	0	7	0	Identify department(s) and key individual(s) responsible for affiliations and partnerships.		
89	7	2	0	8	0	Identify department(s) and key individual(s) responsible for regulatory compliance.		
90	7	2	0	9	0	Identify department(s) and key individual(s) responsible for contract reviews.		
91	7	2	0	10	0	Identify department(s) and key individual(s) responsible for determining technology resource needs.		
92	7	2	0	11	0	Identify department(s) and key individual(s) responsible for marketing related activities.		
93	7	2	0	12	0	Identify department(s) and key individual(s) responsible for network administration and provide a description of responsibilities.		
94	7	2	0	13	0	Identify department(s) and key individual(s) responsible for the performance of system administration and provide a description of responsibilities.		
95	7	2	0	14	0	Identify department(s) and key individual(s) responsible for information security and provide a description of responsibilities.		
96	7	2	0	15	0	Identify department(s) and key individual(s) responsible for application development and provide a description of responsibilities.		
97	7	2	0	16	0	Identify department(s) and key individual(s) responsible for quality assurance and testing and provide a description of responsibilities.		
98	7	2	0	17	0	Identify department(s) and key individual(s) responsible for the performance of database administration and provide a description of responsibilities.		
99	7	2	0	18	0	Identify department(s) and key individual(s) responsible for member service and provide a description of responsibilities.		
100	7	2	0	19	0	Based upon the responses to questions in this section, does it appear that responsibilities are properly segregated (i.e. the credit union is not relying on one individual to support E-Commerce activities)?		
101	**8**	**System Architecture & Controls**						
102						Objective: To determine whether management has designed and implemented the hardware and software architectures to complement each other and to provide for adequate controls.		
103	8	1	**Hardware Architecture**					

	A	B	C	D	E	F	G	H
1			**Credit Union:**					
2			**Charter #:**					
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
104	8	1	0	1	0	Has management identified and reviewed network infrastructure access points and associated risks and vulnerabilities?		
105	8	1	0	2	0	Does the network topology describe the connection points, services, hardware components, etc., such as? - Connections (Internet, Intranet, Extranet, Remote Dial-up) - Operating systems (UNIX, MVS, Windows NT, Linux, VAX/VMS) - Addressing schemes and protocols used (TCP/IP, IPX, SNA) - Internet Service Providers (MCI, Sprint, ATT) and Connection types (e.g., T1) - Services provided (e.g., E-mail, FTP, Telnet, SMTP, DNS) - Communication protocols (POTS, ISDN, DSL, Cable, Frame Relay)		
106	8	1	0	3	0	Are network components configured based on a tested, approved, and secure baseline?		
107	8	1	0	4	0	Are policies, procedures, and practices in place describing how the network components (such as network servers, web servers, transaction servers, application and content servers, database servers, and electronic mail servers) are configured to ensure the proper amount of security?		
108	8	1	0	5	0	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)?		
109	8	1	0	6	0	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)?		
110	8	1	0	7	0	Do the configuration policies and procedures address enabling and monitoring error logs and system auditing functions?		
111	8	1	0	8	0	Do the configuration policies and procedures address configuring components based upon the security required for the applications installed?		
112	8	1	0	9	0	Do the configuration policies and procedures address removing or disabling unnecessary network and operating system services?		
113	8	1	0	10	0	Do the configuration policies and procedures address implementing the necessary		
114	8	1	0	11	0	Do the configuration policies and procedures address replacing components when necessary?		
115	8	1	0	12	0	Are appropriate controls in place to ensure that member traffic is protected from unauthorized users?		
116	8	1	0	13	0	Are controls in place to ensure that employee Internet access is based on job duties and responsibilities?		
117	8	1	1	**Other Network Devices**				
118	8	1	1	1	0	Are there policies and procedures in place to describe the configuration and maintenance criteria associated with network devices that route or store information on the internal network (e.g., routers, hubs, switches, Firewalls, file servers, etc.)?		
119	8	1	1	2	0	Are there policies and procedures in place to describe the use of File Transfer Protocol (FTP) services?		
120	8	1	1	3	0	Are security controls in place to control logical access to workstations? For example: - Limited access to the workstation directory - Automated "time out" facilities that disable an application session after a given time period - Automated utility that monitors and removes "non-standard" software once detected		
121	8	2	**Software Architecture**					
122	8	2	1	**General**				
123	8	2	1	1	0	Is there a standard in place which addresses how HTML pages are secured to prevent unauthorized changes?		
124	8	2	1	2	0	Does management review transactions to ensure the authentication of the user, the integrity of the data, and confidentiality of transactions?		
125	8	2	2	**Change Management**				
126	8	2	2	1	0	Does the credit union have written change management procedures that address management approval, scheduled upgrades, notification to staff and/or members, testing, and implementation?		
127	8	2	2	2	0	Does the change control documentation provide adequate audit trails and support for any type of software modification?		
128	8	2	2	3	0	Are there policies and procedures in place to handle emergency and temporary software fixes as well as new releases or upgrades?		

	A	B	C	D	E	F	G	H
1					Credit Union:			
2					Charter #:			
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
129	8	2	2	4	0	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?		
130	8	2	2	5	0	Are policies, procedures, and practices in place to maintain compatibility throughout the credit union's system environment?		
131	8	2	2	6	0	Does management ensure that operational, technical, and user documentation is kept current and made available to appropriate personnel?		
132	8	2	3	**System Development Life Cycle [SDLC]**				
133	8	2	3	1	0	Are any of the credit union's E-Commerce applications developed in-house? If not, skip this section.		
134	8	2	3	2	0	Does management use a formal methodology or process to guide the acquisition, development, or maintenance of new or modified software?		
135	8	2	3	3	0	Are all affected parties involved in the development of systems specifications and business requirements?		
136	8	2	3	4	0	Is the Information Security Officer or Group a core member of all development projects?		
137	8	2	3	5	0	Are the application developers involved during the initial design as well as the throughout the SDLC process?		
138	8	2	3	6	0	Are there policies, procedures, and practices in place that address unit, system, integration, and acceptance testing for all new or modified systems?		
139	8	2	3	7	0	Does the credit union maintain separate development, test, and production environments?		
140	8	2	3	8	0	Does management employ adequate version control techniques?		
141	8	2	3	9	0	Is training provided to users when new systems are implemented or existing systems modified?		
142	**9**	**Security Infrastructure**						
143						Objective: To determine whether the credit union has implemented a security strategy and related physical and logical access controls to ensure the adequate protection of credit union and member data at all times.		
144	9	1	**General**					
145	9	1	0	1	0	Have any of the credit union's E-Commerce systems been compromised? If so, describe.		
146	9	1	0	2	0	Has management developed and implemented a comprehensive security policy and program which describe the standards and procedures used to protect the credit union's information assets and member data?		
147	9	1	0	3	0	Does the security policy and program address E-Commerce security-related issues?		
148	9	1	0	4	0	Is the security policy and program regularly reviewed and updated based upon technological or operational changes in the environment?		
149	9	1	0	5	0	Has the ability to administer information security and alter system security parameters been limited to appropriate personnel?		
150	9	1	0	6	0	Are all operating systems appropriately configured to protect critical and sensitive data (e.g., disabling unnecessary services and accounts)?		
151	9	1	0	7	0	Does management maintain a current inventory of all security analysis tools?		
152	9	2	**Security Awareness**					
153	9	2	0	1	0	Is a security awareness program in place?		
154	9	2	0	1	1	Is the program promoted by an Information security Officer/Group or similar individual?		
155	9	2	0	1	2	Are user security-related responsibilities regularly communicated to employees?		
156	9	2	0	1	3	Are employees notified that compliance with security policies and procedures Is constantly monitored?		
157	9	2	0	2	0	Does the security awareness program address E-Commerce?		
158	9	2	0	3	0	Are industry (CERT, Bugtraq, etc.) and vendor advisories monitored and appropriate actions taken to protect the credit union's information assets and member data?		
159	9	3	**Firewalls**					
160	9	3	0	1	0	Has the credit union performed a risk assessment to determine the need for Firewalls?		
161	9	3	0	2	0	If the risk assessment indicated a Firewall is needed, has management installed Firewalls? If no, skip this section.		
162	9	3	0	3	0	Are there policies and procedures in place to address the implementation, configuration, and monitoring of Firewalls?		
163	9	3	0	4	0	What types of Firewalls are in use?		
164	9	3	0	4	1	Packet Filtering,		

	A	B	C	D	E	F	G	H
1					Credit Union:			
2					Charter #:			
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
165	9	3	0	4	2	Application Proxy		
166	9	3	0	4	3	Stateful Inspection		
167	9	3	0	4	4	Other (list)		
168	9	3	0	5	0	What brands of Firewalls are in use?		
169	9	3	0	5	1	Checkpoint		
170	9	3	0	5	2	CyberGuard		
171	9	3	0	5	3	Gauntlet		
172	9	3	0	5	4	Other (list)		
173	9	3	0	6	0	Are there any redundancies in the Firewall configuration?		
174	9	3	0	7	0	Do implemented Firewalls detect and protect against:		
175	9	3	0	7	1	IP spoofing attacks?		
176	9	3	0	7	2	Denial of Service attacks?		
177	9	3	0	7	3	Use of hacker programs like finger, whois, tracert and nslookup?		
178	9	4	**Configuration**					
179	9	4	0	1	0	On the Firewall server, have the operating system settings been reviewed and modified for optimum performance?		
180	9	4	0	2	0	Is an audit log kept of all incoming IP addresses and traffic as well as the services/ports that were accessed, dropped or rejected?		
181	9	4	0	3	0	Are there configuration standards and guidelines associated with settings for the primary Firewall?		
182	9	4	0	4	0	Does the configuration limit services like talk, Internet Relay Chat (IRC) and other similar programs (WINAMP, NET Meeting, Instant Messenger) to designated ports?		
183	9	4	0	5	0	Are secondary or redundant Firewalls configured to specifically address the services for which they have been installed?		
184	9	5	**Routers**					
185	9	5	0	1	0	Is the credit union responsible for managing any routers between the credit union and external sources?		
186	9	5	0	1	1	If so, has the responsibility for the configuration of routers and routing tables been clearly defined?		
187	9	5	0	2	0	Are there any modems connected to credit union routers?		
188	9	5	0	2	1	If so, does the credit unions have policies and procedures in place to monitor the use of and ensure that sensitive data and systems are not compromised?		
189	9	6	**Remote Access**					
190	9	6	0	1	0	Does the credit union allow remote access to its systems? If no, skip this section.		
191	9	6	0	2	0	Are there policies and procedures in place which describe the authorization, authentication, and monitoring of remote access users (i.e., vendors, members, and employees)?		
192	9	6	0	2	1	Is any data communicated to other companies via unsecured modems?		
193	9	6	0	2	2	What methods Are in place to ensure that modems Are not susceptible to unauthorized access?		
194	9	6	0	3	0	Has management created remote access user profiles, and has remote access only been granted based upon job duties and/or business needs ?		
195	9	6	0	4	0	Is vendor access to the credit union's network for diagnostic and/or maintenance activities properly restricted, approved and monitored?		
196	9	6	0	5	0	Is the identity of remote users authenticated to the system through passwords or other authentication techniques?		
197	9	6	0	6	0	Does management employ the proper procedures to detect and deny unauthorized remote access? For example, are remote access logs routinely and actively monitored?		
198	9	7	**Access Controls**					
199	9	7	0	1	0	Do the credit union's policies, procedures, and practices address access controls for the web-based systems and applications?		
200	9	7	0	2	0	Can a member access the credit union's web pages using calls to the raw IP address?		
201	9	7	0	3	0	Is the use of harcoded scripts (on the webservers) containing user names, passwords and schemas explicitly disallowed?		
202	9	7	0	4	0	Is there a standard defining under what conditions warning banners should be used?		
203	9	7	0	5	0	Are warning banners prominently displayed to users accessing the website and network systems?		
204	9	7	0	6	0	Are adequate password administration policies and procedures in place?		
205	9	7	0	7	0	Is a process in place which times a session out, or automatically logs off, as a result of user inactivity?		

	A	B	C	D	E	F	G	H
1					Credit Union:			
2					Charter #:			
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
206	9	7	0	8	0	Are there any situations where password authentication is combined with other authentication techniques (i.e. biometric devices, smart cards, etc.)?		
207	9	8	**Monitoring**					
208	9	8	0	1	0	Has the responsibility for monitoring compliance with the security policies, procedures, and practices been clearly defined?		
209	9	8	0	2	0	Has management implemented procedures and practices to monitor compliance with the stated security policy?		
210	9	8	0	3	0	Have information security tools been activated to record and report security events (such as security violations) as defined in information security policies?		
211	9	8	0	4	0	Are security monitoring reports generated and regularly reviewed?		
212	9	8	0	5	0	Are necessary corrective or disciplinary actions taken when security events occur?		
213	9	9	**Member Authentication**					
214	9	9	0	1	0	Are members required to authenticate themselves to the network through the use of unique PINs or passwords?		
215	9	9	0	2	0	Are members identified to the network using either a:		
216	9	9	0	2	1	Static IP address?		
217	9	9	0	2	2	Dynamic Host Configuration Protocol (DHCP)?		
218	9	9	0	3	0	Is a process in place which times a session out, or automatically logs a user off, as a result of member inactivity?		
219	9	9	0	4	0	Has management implemented adequate procedures to ensure the proper identification of a member before resetting or reissuing a password or PIN?		
220	9	10	**Strong Authentication**					
221	9	10	0	1	0	Is authentication data (usernames, passwords, PINs, etc.) encrypted in the database residing on the authentication server?		
222	9	10	0	2	0	Is authentication data (usernames, passwords, PINs, etc.) encrypted during network transmission?		
223	9	10	0	3	0	Are there any network systems or web applications that use One Time passwords or password that have a short life?		
224	9	10	0	4	0	Is authorized access to sensitive data (such as member accounts or personnel records) logged?		
225	9	10	0	4	1	If so, are the logs regularly reviewed to determine whether the access and use of such data was appropriate?		
226	9	11	**Biometric Devices**					
227	9	11	0	1	0	Has a risk assessment or cost/benefit analysis been performed with regards to the implementation of biometrics?		
228	9	11	0	2	0	Does the credit union use biometrics devices for authentication purposes? If no, skip the remainder of this section.		
229	9	11	0	3	0	Are tolerance levels and policies in place that ensure that the user authentication process is performed correctly?		
230	9	11	0	4	0	Are statistical performance metrics routinely monitored to ensure that the process is performed correctly?		
231	9	12	**Encryption**					
232	9	12	0	1	0	During member sessions, is sensitive data encrypted as it is transmitted or received via the Internet and the credit union's network?		
233	9	12	0	2	0	Are there policies and procedures in place that describe how and when encryption should be used to protect transmitted and stored information? Considerations include: - Criteria (key length, algorithm type) put in place to select the appropriate encryption methodology based on data sensitivity - Key management - Key distribution (issuance, revocation, reissuance) - Key storage (on a server with no connection to outside networks)		
234	9	12	0	3	0	If there are international implications for E-Commerce, has the credit union put safeguards in place to ensure compliance with US government policies and restrictions associated with the exportation of encryption technology?		
235	9	13	**Digital Signatures**					
236	9	13	0	1	0	Does the credit union use digital signatures? If no, skip this section.		

	A	B	C	D	E	F	G	H
1					**Credit Union:**			
2					**Charter #:**			
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
237	9	13	0	2	0	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? Some considerations are as follows: - Are digital signatures issued, managed and/or certified by an external vendor? - Are there procedures dealing with the issuance, renewal and revocation of certificates?		
238	9	13	0	3	0	Are digital signatures used to authenticate the credit union?		
239	9	13	0	4	0	Are digital signatures used to authenticate the members?		
240	9	13	0	5	0	Are digital signatures used to authenticate member transactions?		
241	9	13	0	6	0	Does the use of digital signatures include the following:		
242	9	13	0	6	1	Logging sessions?		
243	9	13	0	6	2	Generating and auditing session reports?		
244	9	13	0	6	3	Following up on unusual session activity or errors?		
245	9	13	0	7	0	Are the current laws being monitored with respect to changes associated with the governance of digital signatures?		
246	9	14	**Certificate Authorities (CA)**					
247	9	14	0	1	0	Does the credit union function as a certificate authority? If no, skip this section.		
248	9	14	0	2	0	Has the credit union performed due diligence with respect to the legal implications of providing a CA function?		
249	9	14	0	3	0	Have CA limitations been established for:		
250	9	14	0	3	1	Number of transactions?		
251	9	14	0	3	2	Transaction types?		
252	9	14	0	3	3	CA expirations?		
253	9	14	0	4	0	Does the credit union provide adequate protection for the servers housing the CA information and directories?		
254	9	14	0	5	0	Does the credit union conform to CA standards established by the Internet Engineering Task Force (IETF) and National Institute of Science and Technology (NIST)?		
255	9	14	0	6	0	Are the hosting certificates properly procured and stored?		
256	9	14	0	7	0	Does the credit union maintain backup copies of the certificates?		
257	9	15	**System Auditing**					
258	9	15	0	1	0	Are the appropriate system auditing and logging functions enabled to capture audit trails related to network components?		
259	9	15	0	2	0	Are system, security, and server logs reviewed on a regular basis to detect inappropriate activity?		
260	9	15	0	3	0	Does management take timely action to address inappropriate activity once detected?		
261	9	16	**Intrusion Detection**					
262	9	16	0	1	0	Are there policies and procedures in place to address intrusion detection?		
263	9	16	0	2	0	Do intrusion detection policies and procedures address escalation procedures?		
264	9	16	0	3	0	Do they address how and when to file a Suspicious Activity Report (Required by NCUA Ltr. #96-CU-3)?		
265	9	16	0	4	0	Are there automated notification processes in place for detected intrusions?		
266	9	16	0	5	0	Are unauthorized attempts to access information resources logged and included in a security violation report?		
267	9	16	0	6	0	Is a qualified individual responsible for the regular monitoring of network traffic for potential intrusions?		
268	9	16	0	7	0	Are intrusion detection logs and reports regularly reviewed and any necessary action taken?		
269	9	16	0	8	0	Does the intrusion detection system generate reports and immediately notify administrators of potential intrusions?		
270	9	16	0	9	0	Has an attack and penetration test ever been performed by credit union staff (such as the internal auditor)?		
271	9	16	0	10	0	Has an attack and penetration test ever been performed by an external party?		
272	9	16	0	11	0	Are penetration tests conducted on a regularly scheduled basis as well as whenever significant changes have occurred within the credit union network?		
273	9	16	0	12	0	Are the groups or individuals performing these tests appropriately bonded?		
274	9	17	**Virus Control**					
275	9	17	0	1	0	Are there policies and procedures in place which addresses virus detection and prevention?		
276	9	17	0	2	0	Do these procedures address:		
277	9	17	0	2	1	Notification of potential virus attacks?		

	A	B	C	D	E	F	G	H
1			Credit Union:					
2			Charter #:					
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
278	9	17	0	2	2	Monitoring for anti-virus updates?		
279	9	17	0	2	3	Distribution of updated anti-virus software and definition data files?		
280	9	17	0	2	4	Prevention of the anti-virus tool from being disabled?		
281	9	17	0	3	0	Is all software and data checked for viruses before being loaded onto the credit union’s systems?		
282	9	17	0	4	0	Have users been trained to scan programs, data files and e-mail?		
283	9	18	**Physical Security**					
284	9	18	0	1	0	Has management included physical security in the overall security policy?		
285	9	18	0	2	0	Does the physical security policy address computing (PCs, printers, software) and non-computing (e.g., confidential papers) assets?		
286	9	18	0	3	0	Does the credit union use fire resistant storage cabinets, boxes, or safes for the storage of computing and non-computing assets?		
287	9	18	0	4	0	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?		
288	9	18	0	5	0	Are there policies and procedures in place describing how access to the workspaces, data center, and other sensitive areas is secured and controlled?		
289	**10**	**Business Continuity**						
290						Objective: To obtain reasonable assurance that appropriate backup, recovery, and contingency plans exist to ensure E-Commerce processes will be restored timely in the event of a disruption.		
291	10	1	**General**					
292	10	1	0	1	0	Has management performed and documented a risk assessment to identify and prioritize the credit union's critical systems, including Internet connectivity and E-Commerce products and services?		
293	10	1	0	2	0	Does management periodically reassess their risk analysis to ensure that critical systems are properly identified and prioritized?		
294	10	1	0	3	0	Does the credit union's business continuity and/or disaster recovery plan address the timely recovery of its E-Commerce activities in the event of a disaster?		
295	10	1	0	4	0	Did management consider environmental risks (i.e., flood, earthquake, tornado, fire) when determining the location of the alternate processing site?		
296	10	1	0	5	0	Has the credit union ever invoked its disaster recovery plan? If so:		
297	10	1	0	6	0	Was the recovery process successful?		
298	10	1	0	7	0	Was the plan modified based upon lessons learned?		
299	10	1	0	8	0	Does management periodically test and update the disaster recovery/business continuity plan to reflect the results of testing as well as significant changes in the information technology environment?		
300	10	1	0	9	0	Does the business continuity plan take into consideration those services provided by outsourced vendors?		
301	10	2	**Backup and Recovery**					
302	10	2	0	1	0	Has management established appropriate backup policies and procedures to ensure the timely restoration of E-Commerce services?		
303	10	2	0	2	0	Do these procedures include the following:		
304	10	2	0	2	1	Systems to be backed up?		
305	10	2	0	2	2	Method/type of backup?		
306	10	2	0	2	3	Frequency of backup?		
307	10	2	0	2	4	Storage of backup media?		
308	10	2	0	2	5	Rotation schedule?		
309	10	2	0	2	6	Restoration procedures?		
310	10	2	0	2	7	Timely notification of staff?		
311	10	2	0	3	0	Does management test the backup restoration procedures on a regular basis to ensure the validity of the data and the process?		
312	10	2	0	4	0	Are employees notified of the system downtime for interruptions in service?		
313	10	3	**Backup Power and HVAC**					
314	10	3	0	1	0	Has management ensured that critical systems are connected to a backup power source?		
315	10	4	**Incident Response**					
316	10	4	0	1	0	Are incident response policies and procedures based upon the criticality of the incident?		
317	10	4	0	2	0	Do the incident response procedures address the loss of service due to cyber crimes?		
318	10	4	0	3	0	Have the incident response procedures ever been invoked?		

	A	B	C	D	E	F	G	H
1			**Credit Union:**					
2			**Charter #:**					
3	**E-Commerce Review Program (EC-2)**							
4	**S#**	**SS#**	**SSS#**	**Q#**	**SQ #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
319	10	4	0	3	1	If so, were the procedures revised as a result of the management's findings?		
320	**11**	**Performance Monitoring**						
321						Objective: To ensure that E-Commerce activities are continuously available and efficiently meet member needs and expectations.		
322	11	0	0	1	0	Do the credit union's policies and procedures establish E-Commerce performance standards for the following areas:		
323	11	0	0	1	1	Target throughput parameters?		
324	11	0	0	1	2	Hardware monitoring procedures?		
325	11	0	0	1	3	Transaction volume, response times, and bandwidth availability vs. bandwidth capacity?		
326	11	0	0	1	4	Minimum information system service agreement levels?		
327	11	0	0	2	0	Does management use automated network system monitoring tools such as Simple Network Management Protocol (SNMP), HP Openview, and BMC Patrol?		
328	11	0	0	3	0	Does management employ load balancing to redirect packets to alternating hosts or networks?		

Cell: F28
Comment: This is applicable, for example, to credit unions with global memberships.

Cell: F44
Comment: It is important for management to perform on-going review of contracts to ensure that changes to vendor systems or services do not expose credit union or member data to unnecessary security concerns.

Cell: F45
Comment: Minimum standards should address the vendors' or business partners' financial stability, business practices and overall ability to remain a going concern.

Cell: F58
Comment: Common application programs provided by CSPs include Common Gateway Interface (CGI), Active Server Page (ASP), JAVA Server Page (JSP), and Other Application Programs and Application Program Interfaces (API).

Cell: F88
Comment: This includes managing vendor relationships and monitoring whether service level agreements are being met.

Cell: F91
Comment: Technology resources include hardware and software.

Cell: F93
Comment: Responsibilities may include network performance monitoring, router configuration and maintenance, IP address management, and problem diagnosis.

Cell: F94
Comment: Responsibilities may include hardware and software performance; operating system management and maintenance; new application installation; user account management; and problem diagnosis

Cell: F95
Comment: Responsibilities may include network security, application security and security administration.

Cell: F96
Comment: Responsibilities may include system requirement analysis; system specification; source code development; version control; application distribution and maintenance.

Cell: F97
Comment: Responsibilities might include testing application changes; migrating changes from test to production environment; and maintaining system libraries.

Cell: F98
Comment: Responsibilities might include business modeling; data model design and development;
database location analysis; database sizing requirements; and database schema development.

Cell: F99
Comment: Responsibilities might include responding to member calls for application support; denial of service; and password resets as well as service log and system monitoring.

Cell: F106
Comment: For example, have the following been considered?
- Processor Speed,
- Physical Memory,
- Random Access Memory (RAM),
- Operating System
- Access Control Settings [Read (R),
  Write (W) and Execute (X)]

Cell: G107
Comment: Sample policies, procedures, and practices include: server run with the least privilege userid; access to only a limited portion of the file system (e.g., document or CGI directories); access control lists configured to restrict administrative web page access; server-side interfaces (SSI) configured so dynamic content can not be manipulated by unauthorized parties; and automatic directory index disabled so directory browsing is prevented.

Cell: F109
Comment: This is necessary to keep track of all hardware/software and to ensure compatibility of components.

Cell: F119
Comment: File transfer capabilities should be restricted to ensure that viruses are not introduced via the transfer of files over the Internet.

Cell: F128
Comment: Emergency fixes are necessary due to the severity of problems being addressed. These types of changes should be infrequent.

Cell: F146
Comment: Does the security policy address:
- Data Ownership?
- Confidentiality and protection of credit union and member data?
- Security administration and monitoring responsibilities?
- Authentication techniques?
- Appropriate use of the Internet (including e-mail)?
- Credit union personnel and member responsibilities?
- Threat identification?
- Incident response and notification procedures?
- Exemptions, exceptions and waivers to the policy?
- Disciplinary actions for non-compliance?

Cell: F162
Comment: Some items that should be included are:
- Use of Firewalls
- Timely monitoring for Firewall updates and/or patches
- Timely patch and upgrade implementations
- Documented administrator instructions and procedures
- Restricted physical and physical access to Firewall servers
- Restricted logical access to Firewall configuration rules
- Appropriate testing of all Firewall configuration changes prior to implementation

Cell: F173
Comment: For example, it is not uncommon to have a Firewall in front of and a Firewall behind the same service, such as Firewall between the user and E-mail server and a Firewall between the E-mail server and the mainframe.

Cell: F183
Comment: For example, a Firewall placed in front of the e-mail server, should be properly configured to control e-mail traffic.

Cell: F203
Comment: Such banners should include notice that users are entering or leaving a secured web page, unauthorized use is prohibited, etc.

Cell: F204
Comment: Policies and procedures might address: password length; case sensitivity; password expiration; password change/reset procedures; member identification verification procedures; and password files encryption.

Cell: F215
Comment: 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.

Cell: F219
Comment: For example, secondary authentication methods might include giving a mother's maiden name or sending the PIN to the member's mailing address on file.

Cell: F227
Comment: Biometric devices consist of retina and fingerprint scanners, face scans, etc.

Cell: F247
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.

Cell: F265
Comment: Automatic notification processes include sending emails to designated administrators, paging administrators or security officers, etc.

Cell: F328
Comment: Load balancing is a technique used to alternate traffic between webservers to prevent overloading one or more servers.

	A	B	C	D	E	F
1	**Credit Union:**					
2	**Charter #:**					
3	**Electronic Data Processing Review**					
4	**Sec. #**	**Que. #**	**Sub-Que. #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
5	**1**	**Company Infrastructure**				
6	1	1	**Information Systems Strategy and Planning**			
7				Objective: To obtain reasonable assurance that information systems resources and strategies are sufficient to support the credit union 's overall business objectives and strategies.		
8	1	1	1	Have long and short-term information systems strategies been formulated and approved by management to support the overall business strategy and technology requirements of the credit union ? Does management monitor progress against		
9	1	1	2	Are technical staff's skills and experience required for key positions clearly defined before hiring staff? Does management monitor the adequacy of staffing and related skills and experience?		
10	1	1	3	Are background checks performed when hiring information resource management personnel?		
11	1	1	4	Are key positions supported by succession planning and cross-training?		
12	1	1	5	Are employees given regular performance appraisals?		
13	1	1	6	Is necessary training provided to all technical personnel, and is such training monitored by management and based on regular performance assessments?		
14	1	2	**Relationship with Outsourced Vendors**			
15				Objective: To obtain reasonable assurance that management is appropriately managing outsourced vendor relationships in terms of service levels, pricing, and		
16	1	2	1	Document the credit union 's critical third party processors or outsourced vendors. Indicate the service(s) provided and credit union personnel responsible for managing the relationship.		
17	1	2	2	Does management employ a consistently applied vendor selection process? Does management monitor compliance with this process?		
18	1	2	3	Do selected vendors have to be approved by information technology and appropriate user management?		
19	1	2	4	Are service level metrics defined and agreed to by the affected parties?		
20	1	2	5	How does management monitor vendors' service levels? Is corrective action initiated if performance does not meet expectations?		
21	1	3	**Business Continuity Planning**			
22				Objective: To obtain reasonable assurance that appropriate backup, recovery, and contingency plans exist to ensure critical business processes will be restored in the		
23	1	3	1	Has management established and documented a Disaster Recovery Plan to ensure that essential information systems can be recovered in a timely manner? Is the plan regularly tested and updated?		
24	1	3	2	Has management established and documented a Business Continuity Plan to ensure that essential, non-systems related business processes can be recovered in a timely manner? Is the plan regularly tested and updated?		
25	1	3	3	Do management and the users schedule the backup and retention of data as well as the erasure and release of media when retention is no longer required? Does management periodically review retention and release records?		
26	1	3	4	Is the readability of backup data periodically tested through restoration or other methods?		
27	1	3	5	Are backup media stored off-site and/or in a secure, environmentally controlled location?		
28	1	3	6	Are backup media labeled to enable proper identification?		
29	**2**	**IT Infrastructure**				
30	2	1	**Information Systems Operations**			
31				Objective: To obtain reasonable assurance that computer operations activities provide scheduled, monitored, and secure processing as well as the timely		
32	2	1	1	Has management implemented automated scheduling tools to perform batch processing?		
33	2	1	2	Is access to the job processing software appropriate and based upon user job responsibilities?		
34	2	1	3	Are processing exceptions and errors recorded and reviewed by management?		
35	2	1	4	Has management established a procedure to ensure the system problems are centrally recorded and monitored for timely resolution?		
36	2	1	5	If the credit union has agreement(s) with outside contractors and/or software vendors for technical support, does management monitor for compliance with these agreements?		
37	2	1	6	Does management provide for alternate sources of power (i.e., uninterruptible power supply, generators)?		

	A	B	C	D	E	F
1	Credit Union:					
2	Charter #:					
3	**Electronic Data Processing Review**					
4	**Sec. #**	**Que. #**	**Sub-Que. #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
38	2	1	7	Has management implemented adequate smoke/fire detection and suppression devices?		
39	2	1	8	Are the environmental conditions of the data center (i.e., temperature, humidity) monitored and regulated?		
40	2	2	**Network Support**			
41				Objective: To obtain reasonable assurance that network environment is appropriately maintained.		
42	2	2	1	Does management approve the acquisition and modification of network and communications software and systems to ensure compliance with system plans		
43	2	2	2	Does the credit union use a formal methodology or process to guide the acquisition, development or maintenance of network and communication software?		
44	2	2	3	Is network and communication software/hardware initially installed and evaluated in a test environment before implementation?		
45	2	2	4	Is the timing of changes to network and communication software coordinated with all affected parties to minimize the impact to regular processing activities?		
46	2	2	5	Are network changes performed in a manner that allows the original environment to be restored if necessary?		
47	2	2	6	Does management ensure that supported versions of network and communication software are being used and that new releases are implemented timely?		
48	2	2	7	Does management monitor network performances and ensure a prompt response to inefficient performance?		
49	2	3	**Operating System Support**			
50	2	3		Objective: To obtain reasonable assurance that operating system software within the technical environment is appropriately maintained.		
51	2	3	1	Does management approve the acquisition and modification of operating system software to ensure compliance with system plans and strategies?		
52	2	3	2	Is the timing of changes to operating systems software coordinated with all affected parties to minimize the impact on other processing activities?		
53	2	3	3	Is current documentation for systems software available and used when installing		
54	2	3	4	Are all operating system acquisitions and modifications tested prior to implementation?		
55	2	3	5	Are vendor-issued operating system changes obtained from the vendor and implemented in a timely manner to ensure on-going support?		
56	2	3	6	Are backout procedures for operating system changes developed and documented to allow the original environment to be restored is necessary?		
57	2	3	7	Are operating system changes tested to ensure that applications are not adversely affected by the changes?		
58	2	3	8	Does management review operating system performance to ensure that adequate action is taken upon identification of inefficient performance?		
59	2	4	**Hardware Support**			
60	2	4		Objective: To obtain reasonable assurance that hardware within the technical environment is appropriately maintained.		
61	2	4	1	Does management approve the acquisition and modification of computer hardware to ensure compliance with the credit union 's system plans and strategies?		
62	2	4	2	Is computer hardware initially installed and evaluated in a test environment before		
63	2	4	3	Are replacement parts and/or service readily available for computer hardware?		
64	2	4	4	Does the computer hardware include self-diagnostic routines capable of alerting management or the appropriate vendor to potential problems or malfunctioning parts?		
65	2	5	**Application Development and Maintenance**			
66	2	5		Objective: To obtain reasonable assurance that changes to application systems are appropriately initiated, tested, approved, and migrated to the production environment.		
67	2	5	1	Does management approve all decisions to purchase or develop application systems in order to ensure consistency with organizational plans and strategies?		
68	2	5	2	Does the credit union use a formal methodology or process to guide the acquisition, development or maintenance of application systems?		
69	2	5	3	Are application systems developed, modified, and tested in an environment separate from the production environment?		

	A	B	C	D	E	F
1	**Credit Union:**					
2	**Charter #:**					
3	**Electronic Data Processing Review**					
4	**Sec. #**	**Que. #**	**Sub-Que. #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
70	2	5	4	Is access to the test and production environments appropriately restricted?		
71	2	5	5	Is the timing of changes to application systems coordinated with all affected parties to minimize the impact on other processing activities?		
72	2	5	6	Do system implementation procedures include training users on appropriate use of new or substantially modified systems? Is compliance with these procedures monitored by management?		
73	2	5	7	Is application source code as well as technical and user documentation maintained for executable production programs?		
74	2	5	8	Does management review and approve the conversion of data (e.g., balancing and reconciliation activities) from old application systems to new systems?		
75	2	5	9	Does management retain prior versions of application systems and/or data to allow for recovery of the environment in the event of processing problems?		
76	2	5	10	If the credit union has formal agreements with outside vendors to obtain application support, does management monitor compliance with these agreements?		
77	2	5	11	Does management ensure that supported versions of purchased application systems are being used and that new releases are implemented timely?		
78	2	5	12	Is the development staff adequately trained and familiar with the common set of standards, technology and tools used by the organization?		
79	2	7	**Database Support**			
80	2			Objective: To obtain reasonable assurance that database software is appropriately maintained.		
81	2	7	1	Is responsibility for administration and definition of database components assigned to appropriate personnel?		
82	2	7	2	Does management approve all decisions to purchase or modify data structures to ensure consistency with organizational systems plans and strategies?		
83	2	7	3	Are modifications to the data structure evaluated in a test environment before implementation?		
84	2	7	4	Do procedures exist to ensure all affected parties are contacted before significant changes are made to data structures and the timing of such changes have minimal impact on operations?		
85	2	7	5	Does the credit union ’s database management system include an active data dictionary that is automatically updated for changes to the database?		
86	2	7	6	Does management monitor database performance and take appropriate corrective actions, when necessary?		
87	**3**	**Security Infrastructure**				
88	3	1	**Information Systems Security**			
89				Objective: To determine whether the credit union has implemented a security strategy and related physical and logical access controls to ensure the adequate protection of credit union and member data at all times.		
90	3	1	1	Has management established and documented an adequate information security policy to provide for the overall direction and implementation of information security?		
91	3	1	2	Are the roles and responsibilities related to information security administration appropriately defined and assigned?		
92	3	1	3	Has the ability to administer information security and make modifications to overall system security parameters been limited to appropriate personnel? Is the use of privileged accounts ("administrator" or "superuser") limited to appropriate personnel, logged and reviewed?		
93	3	1	4	Have information security tools been activated to record and report security events (such as security violation reports) as defined in information security policies? Are these reports regularly reviewed and necessary corrective and disciplinary actions taken?		
94	3	1	5	Have vendor default passwords for operating system, application, communication and network software been modified?		
95	3	1	6	Are terminals and workstations used to process sensitive data protected by time-out facilities that are activated after a predetermined time period of inactivity?		
96	3	1	7	Is sensitive data encrypted while being transmitted over the credit union ’s network?		

	A	B	C	D	E	F
1	**Credit Union:**					
2	**Charter #:**					
3	**Electronic Data Processing Review**					
4	**Sec. #**	**Que. #**	**Sub-Que. #**	**Audit Program Step**	**Y/N/ NA/ NR**	**Comments**
97	3	1	8	Is the identity of users (both local and remote) authenticated to the system through passwords or other authentication techniques? Does the use of passwords incorporate policies on periodic change, confidentiality and password format (e.g. password length, alphanumeric content)?		
98	3	1	9	Are unauthorized attempts to access information resources logged and reported? Are the logs and reports regularly reviewed and necessary corrective action taken?		
99	3	1	10	Are access privileges immediately changed for employees who have changed responsibilities or been terminated?		
100	3	1	11	Is anti-virus software resident on all credit union ’s computers and on any computer that is allowed to connect to the organization’s network? Is the software scanned for viruses whenever downloading data or programs, opening data files, or executing programs?		
101	3	1	12	Are users required to periodically update the virus signature lists on their computers?		
102	3	1	13	Are controls in place which ensure that all software loaded on company computers is properly authorized and licensed? If unlicensed or unauthorized software is found, is appropriate action taken?		
103	3	1	14	Are appropriate physical restrictions in place for protected areas? Is the authority to modify physical access controls limited to appropriate personnel?		

	A	B
1	**Term**	**Definition**
2	**Access Control Entry (ACE)**	Each access control list has an associated ACE, which lists the permissions that have been granted or denied to the users or groups listed in the ACL.
3	**Access Control List (ACL)**	List of security identifiers that allow only certain processes to be activated.
4	**Access Products**	Products that allow consumers to access traditional payment instruments electronically, generally from remote locations.
5	**Access Tokens**	Objects containing the security identifier of a running process. The access token is checked against each object’s ACL to determine whether or not appropriate permissions are granted.
6	**Acquirer**	In an electronic money system, the entity or entities (typically banks) that hold deposit accounts for merchants and to which transaction data are transmitted.
7	**Administrative Alerts**	When a computer generates an alert, the message is sent to a predefined list of users. These messages relate to server and resource use; they warn about problems in areas such as security and access, user sessions, server shutdown because of power loss (with UPS), directory replication, and printing.
8	**Alerter Service**	Notifies selected users and computers of administrative alerts that occur on a computer.
9	**Algorithms**	Mathematical formulas used to encrypt and decrypt messages. These encryption formulas can reside in software or specialized hardware devices.
10	**Alpha Test**	The first stage of testing a new software product, carried out by the manufacturer’s staff.
11	**Alternative Payment Systems**	Payment systems such as those based on stored value cards, electronic currency, and debit or credit cards. These are alternative avenues to deliver traditional banking and related products and services.
12	**American National Standards Institute (ANSI)**	A standard setting organization; it is the U.S. representative to the International Standards Organization (ISO).
13	**American Standard Code for Information Interchange (ASCII)**	A standard code for representing characters as numbers that is used on most microcomputers, computer terminals, and printers.
14	**Applet**	A small application program that is designed to do a small, specific job.
15	**Application**	A computer program or set of programs that perform the processing of records for a specific function.
16	**Asymmetric Cryptography**	Is also known as public/private key cryptography. A private key encrypts the data and a public key decrypts the information. Asymmetric cryptography is slower than symmetric technology and is used primarily for message authentication purposes.
17	**Asynchronous Transfer Mode (ATM)**	Method of transmitting bits of data one after another with a start bit and a stop bit to mark the beginning and end of each data unit.
18	**Audit Policy**	Defines the type of security events that are logged for a domain or for individual computers; determines what the operating system will do when the security log becomes full. Audit policy can track the success or failure of specified security events.
19	**Auditability**	The degree to which transactions can be traced and audited through a system.
20	**Authentication**	1) The process which assures the receiver of a digital message of the identity of the sender. It also is used to validate the integrity of the message. 2) The process of proving the claimed identity of an individual user, machine, software component or any other entity.
21	**Authoring Software**	Software used to produce multimedia or hypertext presentations by linking sounds, music, visuals, and text.
22	**Authorization**	The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity.
23	**Automated Clearing House (ACH)**	An automated clearing and settlement system for recurring payments. Most ACH systems are operated by the Federal Reserve Banks.
24	**Backdoor**	A hole or access point left, by design, in the program by the original programmer or developer. Usually used by programmers to simplify the program-testing procedures; however, on occasion, programmers forget to. close these holes or are not aware of other holes created by the original backdoor.
25	**Bandwidth**	The transmission capacity of a computer channel or communications line.
26	**Bastion Host**	A firewall system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack. Bastion hosts are often components of firewalls, or may be “outside” web servers or public access systems.
27	**Baud Rate**	Measurement of data transfer speed.
28	**Beta Test**	The second stage of a new software product that is almost ready for market, typically carried out by volunteers in a wide variety of settings such as those in which the finished product will be used.
29	**Biometrics**	A method of verifying an individual’s identity by analyzing a unique physical attribute.
30	**BIT**	A binary digit (0 or 1) used in the representation of a number, letter, or special character.

	A	B
31	**Bridge**	In local area networks, a device that enables two networks, even ones dissimilar in topology, wiring, or communications protocols, to exchange data.
32	**Browser**	A computer program that enables the user to retrieve information that has been made publicly available on the Internet; also permits multimedia (graphics) applications on the World Wide Web.
33	**Browser**	A computer program that enables the user to retrieve information that has been made publicly available on the Internet; also that permits multimedia (graphics) applications on the World Wide Web.
34	**Bundled Software**	Software that is sold in combination with hardware.
35	**CERT**	See Computer Emergency Response Team
36	**Certifying Authority**	A trusted third party that confirms a person’s identity by certifying that the transaction belongs to the stated party. The certifying authority must be recognized, trusted, and protected from fraud and abuse. A certifying authority issues a digital certificate signed by their private key. It can be verified by decrypting the certificate using the authority’s public key.
37	**Chip**	An electronic device consisting of circuit elements on a single silicon chip. The most complex circuits are microprocessors, which are single chips that contain the complete arithmetic and logic units of computers.
38	**Chip Card**	Also known as an integrated circuit (IC) card. A card containing one or more computer chips or integrated circuits for identification, data storage, or special-purpose processing used to validate personal identification numbers, authorize purchases, verify account balances, and store personal records.
39	**Cipher Text**	An encrypted message that outsiders cannot read.
40	**Clearing**	The process of transmitting, reconciling and, in some cases, confirming payment orders prior to settlement, possibly including netting of instructions and the establishment of final positions for settlement.
41	**Clearing House**	A central location or central processing mechanism through which financial institutions agree to exchange payment instructions. The institutions settle for items exchanged at a designated time, based on the rules and procedures of the clearing house.
42	**Clearing System**	A set of procedures whereby financial institutions present and exchange data and/or documents relating to funds or securities transfers to other financial institutions.
43	**Client Server Network**	A method of allocating resources in a local area network so that computing power is distributed among computer workstations in the network but some shared resources are centralized in a file server. These networks dedicate certain computers called servers to act as service providers to computers called clients.
44	**Closed Network**	A telecommunications network that is used for a specific purpose, such as a payment system, and to which access is restricted (also referred to as a private network).
45	**Closed Stored Value System**	A system in which value is issued and accepted by either a relatively small group of merchants, or in which the system is limited geographically (i.e., university programs and fare cards for mass transit systems).
46	**Code**	Computer programs, written in machine language (object code) or programming language (source code).
47	**Computer Emergency Response Team (CERT)**	Located at Carnegie-Mellon University, this incident response team offers advisories that contain useful, specific security information.
48	**Cracker**	A computer operator who breaks through a system’s security. This can be legitimate activity, such as to test system security measures.
49	**Cryptography**	The principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form (i.e., scrambling a message).
50	**Cyber Mall**	A set of electronic or digital storefronts linked through a common Web site.
51	**Cyberspace**	A popularized term that refers to the part of society and culture that exists in networked computer systems rather than in any particular physical location.
52	**Data Encryption Standard (DES)**	U.S. government standard for data encryption method published by the National Institute of Standards and Technology for the encryption of sensitive U.S. government data which does not fall under the category of national security related information. The DES uses a 64 bit key.
53	**Data Integrity**	The property that data meet with a priority expectation of quality and that the data can be relied upon.
54	**Database Administrator (DBA)**	The individual with authority to control the data base management system.
55	**Dedicated**	Assigned to only one function.
56	**Default Shares**	Resources shared by default when the operating system is installed.
57	**Denial- of- Service Attack**	An attempt to overwhelm a server with requests so that it cannot respond to legitimate traffic.
58	**Design Phase**	The phase during which the problem solution that was selected in the Study Phase is designed. The design includes the allocation of system functions; the design of inputs, outputs, and files; and the identification of system and component requirements.

	A	B
59	**Design Specification**	A baseline specification that defines how to construct a computer based business system.
60	**Development Phase**	The phase in which the computer based system is constructed from the “blueprint” prepared in the Design Phase. Equipment is acquired and installed. All necessary procedures, manuals, and other documentation are completed. Personnel are trained, and the complete system is tested for operational readiness.
61	**Dialup**	The ability of a remote user to access a system by using private or common carrier telephone lines.
62	**Dial-up Client**	A computer with a temporary connection to the Internet.
63	**Digital**	Referring to communications processors, techniques, and equipment where information is encoded as a binary “1”or “0”.
64	**Digital Certification**	A process to authenticate (or certify) a party’s digital signature; carried out by trusted third parties.
65	**Digital Envelope**	A digital message protected by a digital signature.
66	**Digital Signature**	1) A mathematical encryption technique that associates a specific person with a given computer file and indicates that the file has not been altered since that person signed it; should not be confused with making an electronic representation of a written signature. 2) A message digest encrypted using asymmetric cryptography. This is used to verify that a message came from the expected sender.
67	**Distributed Transaction Processing**	Application processing that involves multiple users requiring concurrent access to a single shared resource.
68	**Domain**	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
69	**Domain Controller**	The server that authenticates domain logins and maintains the security policy.
70	**Domain Name**	An alphanumeric name for a Web site that includes both the online address and online name.
71	**Domain Name Service (DNS)**	A network service that translates external Internet addresses into numerical Internet network addresses.
72	**Double Spending (Respending)**	Creating and spending copies of stored value files.
73	**Download**	To transmit a file or program from a central computer to a smaller computer or to a remote site.
74	**Dynamic Host Configuration**	Method of automatically assigning addresses to client computers on a network.
75	**Electronic Benefits Transfer (EBT)**	The electronic delivery of government benefits, using plastic cards and available ATM and point of sale (POS) technology.
76	**Electronic Cash**	The digital equivalent of dollars and cents (also referred to as digital cash).
77	**Electronic Data Interchange (EDI)**	The transfer of information between organizations in machine readable form.
78	**Electronic Document**	The digital or computer equivalent of paper documents.
79	**Electronic Money**	Monetary value measured in currency units stored in electronic form on an electronic device in the consumer’s possession. This electronic value can be purchased and held on the device until reduced through purchase or transfer.
80	**Electronic Purse**	A stored value device that can be used to make purchases from more than one vendor.
81	**Email**	Messages people send to one another electronically from one computer to another.
82	**Encryption (Cryptography)**	The process of scrambling data by a device or encoding principle (mathematical algorithms) so that the data cannot be read without the proper codes for unscrambling the data.
83	**End-to-end Encryption**	The protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.
84	**Ethernet**	A type of local area network originally developed by Xerox, communication takes place by means of radio frequency signals carried over coaxial cable.
85	**Feasibility Analysis**	The process of determining the likelihood that a proposal will fulfill specified objectives.
86	**File Transfer Protocol (FTP)**	A standard way of transferring files from one computer to another on the Internet.
87	**Firewall**	A system or combination of hardware and software solutions that enforces a boundary between two or more networks.
88	**Flowchart**	A programming tool to graphically present a procedure by using symbols to designate the logic of how a problem is solved.
89	**Gamma Test**	The third stage of software testing completed before release.
90	**Gateway**	1) A computer that performs protocol conversion between different types of networks or applications. 2) A computer that serves as a router, a format translator, or a security filter for an entire network.
91	**Gopher**	A computer program, and an accompanying data transfer protocol, for reading information that has been made available to users on the Internet.
92	**Graphical User Interface (GUI)**	A way of communicating with a computer by manipulating icons (pictures) and windows with a mouse.

	A	B
93	**Group Identifiers**	Security identifiers that contain a set of permissions given to a given group of users. All of the users in that group have the permissions granted to that group. Groups Security identifiers to which users can be assigned membership for the purpose of applying a broad set of group permissions to the user. This allows for better management and control over large security environments.
94	**Groupware**	Software that allows a group of users to work on the same data through a network by facilitating file sharing and other forms of communication.
95	**Hacker**	A computer operator who breaks into a computer without authorization, for malicious reasons, just to prove it can be done, or other personal reasons.
96	**Hardware Compatibility**	A listing of all hardware devices supported by the operating system.
97	**Hash Function**	Used to create a message digest. The sender of a message uses a hash function to derive a calculation from a particular message.
98	**Heterogeneous Networks**	Networks consisting of a variety of computer systems. Typically, these types use the TCP/IP (transmission control protocol/Internet protocol) network communication protocol to get these systems operating together. Managing a heterogeneous network is difficult since each operating system has its own security system. How these operating systems interact as a whole will determine the effectiveness of the security system.
99	**Home Banking**	Banking services that allow a customer to interact with a financial institution from a remote location by using a telephone, television set, terminal, personal computer, or other device to access a telecommunication system which links to the institution’s computer center.
100	**Home Page**	A screen of information made available to users through the Internet or a private Intranet; it is the “main page” that users are expected to read first in order to access the other pages that comprise the Web site.
101	**Host**	Also known as a host computer that is the primary or controlling computer in a computer network, generally involving data communications or a local area network.
102	**Hypertext**	Electronic documents that present information that can be connected together in many different ways, instead of sequentially.
103	**Hypertext Markup Language (HTML)**	A set of codes that can be inserted into text files to indicate special typefaces, inserted images, and links to other hypertext documents.
104	**Hypertext Transfer Protocol (HTTP)**	A standard method of publishing information as hypertext in HTML format on the Internet.
105	**Icon**	A small picture on a computer screen that represents a particular object, operation, or group of files.
106	**IDEA**	International Data Encryption Algorithm.
107	**IETF**	Internet Engineering Task Force: a standards-setting organization.
108	**Incident Response Team**	A team of computer experts (internal or external) organized to protect an organization’s data, systems, and other assets from attack by hackers, viruses, or other compromise.
109	**Integrated Circuit Card (IC Card)**	A plastic card in which one or more integrated circuits are embedded (also called a chip card).
110	**Integrated Services Digital Network (ISDN)**	A type of all digital telephone service. Isdn lines provide a connection that can transmit digital data as well as voice, without a modem.
111	**International Organization for Standardization/Open Systems Interconnection (ISO/OSI)**	An international standard setting organization. ANSI is the U.S. representative.
112	**Internet**	A worldwide network of computer networks (commonly referred to as the Information Superhighway).
113	**Internet Information Server**	Software used to serve higher-level Internet protocols, like HTTP and FTP for clients using Web browsers.
114	**Internet Service Provider (ISP)**	An entity that provides access and/or services related to the Internet, generally for a fee.
115	**Interoperability**	The compatibility of distinct applications, networks, or systems.
116	**Intranet**	A private network that uses the infrastructure and standards of the Internet and World Wide Web, but is cordoned off from the public Internet through firewall barriers.
117	**ISDN**	Integrated Services Digital Network. A type of all-digital telephone service that can transmit digital data as well as voice, without a modem.
118	**Issuer**	In a stored value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it.
119	**Kernel**	The core process of a preemptive operating system, generally consisting of a multitasking scheduler and the basic security services.
120	**Key**	1) The integers that drive the encryption algorithm. 2) A secret value or code used in an encrypting algorithm known by one or both of the communicating parties.
121	**Large dollar Funds Transfer System**	A funds transfer system through which large dollar and high priority funds transfers are made between participants in the system for their own account or on behalf of their customers. Sometimes known as wholesale funds transfer systems.

	A	B
122	**Limited Purpose Prepaid Card**	A prepaid card which can be used for a limited number of well defined purposes. Its use is often restricted to a number of identified points of sale within a specified location. In the case of single purpose prepaid cards, the card issuer and the service provider may be identical.
123	**Local Area Network (LAN)**	A network that connects several computers that are located nearby (in the same room or building), allowing them to share files and devices such as printers.
124	**Lock and Key Protection System**	A protection system that involves matching a key or password with a specific access requirement.
125	**Logging**	The storing of information about events that occurred on the firewall or network.
126	**Logon Script**	Command files that automate the logon process by performing utility functions such as attaching to. additional server resources or automatically running different programs based on the user account that established the logon.
127	**Long File Name (LFN)**	A filename longer than the MS-DOS allowed eight plus extension. In Windows NT, windows 98/95, OS/2, Unix, and Linux, for example.
128	**Magnetic Stripe**	Used on debit, credit, and identification cards to store encoded information read by card readers; less secure than computer chip cards.
129	**Memory Card**	An integrated circuit (IC) card capable of storing information only.
130	**Message Digest**	A value created from a hash function. This value is known as the message digest. The receiver can verify the value to determine whether any changes were made to the message during transmission.
131	**Middleware**	Facilitates the client/server connections over a network and allows client applications to access and update remote databases and mainframe files.
132	**Multimedia**	The combining of different elements of media (i.e., text, graphics, audio, video) for display and control from a personal computer.
133	**Multiprocessing**	Using two or more processors simultaneously to perform a computing task. Normally a hardware level capacity to perform this function: C Asymmetrically: Certain processors are assigned certain threads independent of the load they create. C Symmetrically: Threads are dynamically assigned to processors according to an equitable scheduling scheme.
134	**Multipurpose Prepaid Card**	A prepaid card which can be used for a wide range of purposes and has the potential to be used on a national or international scale but may sometimes be restricted to a certain area.
135	**Multitasking**	The ability of a processing unit to switch rapidly among threads of execution. Multitasking divides processor time among threads as if each thread ran on its own slower processor. These systems allow two or more applications to run at the same time and can provide a greater degree of service to applications than single-tasking operating systems.
136	**National Institute for Standards and Technology (NIST)**	Established within the Department of Commerce to develop technical, management, physical and administrative standards and guidelines for the cost effective security and privacy of sensitive information in Federal computer systems. NIST issues the Federal Information Processing Standards (FIPS).
137	**National Security Agency (NSA)**	Responsible for government and/or military information security.
138	**National Telecommunications Information Administration (NTIA)**	A government agency charged with safeguarding personal information on U.S. citizens.
139	**Navigation**	Moving through a complex system of menus or help files.
140	**Network**	A group of computers connected by cables or other means and using software that enables them to share equipment and exchange information. A system of software and hardware connected in a manner to support data transmission.
141	**New Technology (NT)**	A Microsoft operating system.
142	**Newsgroup**	Public forums or discussion areas on a computer network; generally topic focused.
143	**Node**	Any device, including servers and workstations, connected to a network. Also, the point where devices are connected.
144	**Non-repudiable Transactions**	Transactions that cannot be denied after the fact.
145	**Nonrepudiation**	The undeniable proof of participation by both the sender and the receiver in a transaction. It is the reason public key encryption was developed, i.e., to authenticate electronic messages and later prevent denial or repudiation by the sender or receiver.
146	**NT File System (NTFS)**	A secure, transaction-oriented file system developed for Windows NT allowing assignment of permissions and shares with access limited to properly authenticated users.
147	**Object**	A self-contained entity that contains its own data and the functions necessary to manipulate the data. NT’s security system controls access to objects and the audit system logs them.
148	**Offline**	Equipment or devices that are not in direct communication with the central processor of a computer system, or connected only intermittently.

	A	B
149	**Online**	Equipment or devices that communicate with a computer network. Connections can be direct (as in a LAN using dedicated connections) or indirect (as in using the internet).
150	**Online Scrip**	Debit accounts on the Internet or other major computer network.
151	**Online Service Providers (OSP)**	Closed network services that provide access to various computer sites or networks for a fee.
152	**Open Network**	A data communications network to which access is not restricted.
153	**Open Stored Value System**	A system that may be comprised of one or more electronic cash issuers of stored value that is accepted by multiple merchants or entities.
154	**Operating System**	1) A collection of services that form a foundation upon which applications run. Examples include: MS-DOS: A simple I/O service provider with a command shell and Windows NT: A sophisticated, preemptive, multitasking, multiprocessing application platform. 2) A program that controls a computer and makes it possible for users to enter and run their own programs.
155	**Operation Phase**	The phase in which changeover from an old system to a new system occurs. The system is then operated and maintained. System performance is audited, and change to the system is managed.
156	**Ownership**	The owner of a file or directory has control of that file or directory and can change its permissions. By default, the user who creates the file or directory owns it.
157	**Packet Switching**	A data transmission method that routes packets along the most efficient path and allows a communication channel to be shared by multiple connections.
158	**Password**	A unique word or string of characters that a programmer, computer operator, or user must supply to satisfy security requirements before gaining access to the system or data.
159	**Password Cracker**	A software program designed to conduct an automated brute force attack on the password security controls of an information system by “guessing” user passwords.
160	**Password Sniffer**	A software program that is illicitly inserted somewhere on a network to capture user passwords as they pass through the system.
161	**Payment System**	A financial system that establishes the means for transferring money between suppliers and users of funds, usually by exchanging debits or credits between financial institutions.
162	**Penetration Testing**	Using automated tools to determine a network’s vulnerability to unauthorized access.
163	**Performance Specification**	A baseline specification that describes what a computer-based business system is to do. It is completed at the conclusion of the study phase.
164	**Permission**	A rule associated with an object to regulate which users can access the object and in what manner.
165	**Personal Identification Number (PIN)**	A sequence of digits used to verify identity.
166	**Personal User Profile**	A profile created by the administrator and assigned to a user. This records changes the user makes to their operating system or network environment settings. This is saved when the user logs off, and is loaded when the user logs on.
167	**PGP**	Pretty Good Privacy data encryption algorithm.
168	**Piggyback**	A means of gaining unauthorized access to a system through another user’s legitimate connection.
169	**Plain Text**	An unencrypted message.
170	**Point of Sale (POS)**	A system of terminals that debits or charges a customer’s account and credits or pays a merchant’s account to effect payment for purchases at retail establishments.
171	**Point-to-Point Tunneling**	Supports a secure, multi-protocol private network across the Protocol Internet. Makes use of authentication and encryption to secure communications. Windows NT supports this function by its remote-access service (RAS).
172	**Policies**	General controls that enhance the security of an operating environment. For example, policies could affect restrictions on password use and rights assignments and determine which events will be recorded in the security log.
173	**Prepaid Card**	A card on which value is stored, and for which the holder has paid the issuer in advance.
174	**Priority**	A level of execution importance assigned to a thread. In combination with other factors, the priority level determines how often that thread will get computer time according to a scheduling algorithm.
175	**Privacy**	In the context of a payment system, the property that no information which might permit determination of transactions may be collected without the consent of the counter parties involved.
176	**Privacy-Enhanced Mail (PEM)**	An Internet standard for secure electronic mail. The standard adds several security services to the Internet electronic mail messages: message origin authentication; message integrity; nonrepudiation of origin; and message confidentiality.
177	**Private Branch Exchange**	A computer system that drives the internal telephone (PBX) system in an organization. The PBX is connected to the telephone company and possibly other networks.

	A	B
178	**Protocols**	1) A standardized set of rules that define how computers communicate with each other. 2) An established rule of communication adhered to by the parties operating under it.
179	**Proximity Cards**	Cards that can be read from a short distance; mainly used for security and vehicle identification.
180	**Public Key Cryptography**	A two-key method of cryptography where a non-public key is used to encode and a second, publicly available key is used to decode. Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.
181	**Public Law 100-235**	Computer Security Act of 1987; assigned the National Institute of Standards and Technology with the responsibility for developing standards and guidelines for federal computer systems processing unclassified data.
182	**Real Time Monitoring**	The monitoring of activity as it occurs rather than storing the data for later review.
183	**Registry**	A database repository for information about a computers configuration, including the hardware, installed software, environment settings, and other information.
184	**Remote Access**	Letting off-site users access a central network.
185	**Remote Payment**	A payment carried out through the sending of payment orders or payment instruments.
186	**Remote Procedure Calls**	A network interprocess communication mechanism that allows an application to be distributed among many computers on the same network.
187	**Repudiation**	The denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication.
188	**Requests for Comments**	The set of standards defining the Internet protocols by the Internet Engineering Task Force and available in the public domain on the Internet. RFCs define the functions and services provided by each of the many Internet protocols. Compliance with the RFCs significantly enhances cross-vendor compatibility.
189	**Router**	A computer system in a network that stores and forwards data packets between local area networks and wide area networks.
190	**RSA**	A public key (asymmetrical) encryption methodology. It was invented in 1976 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is used as a supplement to DES. It provides for secure key exchanges and digital signatures. Key lengths can vary from 40 to 1,024 bits.
191	**Scalability**	The ability of a system to support high-growth enterprise applications. These applications are typically large-scale, mission-critical in nature. Examples include supporting widely used online banking activities, hosting popular Web sites, maintaining large data warehouses, and administering large e-mail systems.
192	**Scattering**	The process of mixing the integrated circuit (IC) chip components so that they cannot be analyzed easily.
193	**Search Engines**	Software programs that are capable of locating specified information or Web sites on the Internet.
194	**Searchware**	Software used to search through a database.
195	**Secure Electronic Transaction (SET)**	A set of standards jointly developed by Visa, MasterCard, and several technologies companies to facilitate secure credit card transactions over the Internet.
196	**Secure Hypertext Transfer Protocol (SHTTP)**	Provides secure communication mechanisms between an HTTP client-server pair.
197	**Secure Socket Layer (SSL)**	A protocol for providing data security during transmission using data encryption, server authentication, and message integrity.
198	**Security Accounts Manager**	The module of the NT executive that authenticates a user name and password against a database of accounts, generating an access token that includes users' permissions.
199	**Security Identifiers (SIDs)**	Unique codes that identify a specific user or group to the NT security system. SIDs contain a complete set of permissions for that user or group.
200	**Security Policies**	The security policy consists of the Account, User Rights, Audit, and Trust Relationships policies, and are managed with User Managers for Domains.
201	**Server**	1) A computer dedicated to servicing requests for resources from other computers on a network. Servers typically run network operating systems. 2) A computer that provides services to another computer (the client).
202	**SET**	A set of standards jointly developed by Visa, MasterCard, and several technologies companies to facilitate secure credit card transactions over the Internet. Secure Electronic Transactions is a standard developed by VISA and MasterCard. SET uses public key cryptography and requires merchants and consumers to have authentication keys to conduct online transactions. The purpose is to secure transactions over open networks such as the Internet.
203	**Settlement**	An act that discharges obligations with respect to funds or securities transfers between two or more parties.
204	**Settlement System**	A system used to facilitate the settlement of transfers of funds.
205	**Simple Mail Transfer Protocol (SMTP)**	A protocol used to transfer electronic mail between computers on the Internet.

	A	B
206	**Smart Card**	A card with a computer chip embedded, on which financial, health, educational, and security information can be stored and processed.
207	**Social Engineering**	Posing as managers, technicians, or other employees to gain access to computer resources either directly by corporate or by obtaining access codes or access from authorized users.
208	**Specification**	Documents that contain basic detailed data.
209	**Spoofing**	An attempt to gain access to a system by posing as an authorized user.
210	**Standards**	The rules under which analysts, programmers, operators, and other personnel in an information service organization work.
211	**Stored Value Card**	A card that stores prepaid value via magnetic stripe or computer chip.
212	**Structured Query Language (SQL)**	A query language used to manipulate large databases.
213	**Structured Walk-through**	A technical review performed to assist the technical people working on a project. It is one of a series of reviews that should be a planned part of system design and development activities.
214	**Study Phase**	The phase during which a problem is identified, possible solutions are studied, and recommendations are made with regard to committing the resources required to design a system.
215	**Subnet Mask**	A number mathematically applied to addresses to determine which addresses are a part of the same subnetwork as the computer applying the subnet mask.
216	**Switch**	A type of bridge that can move several packets at the same time.
217	**Symmetrical**	A private or secret key cryptography methodology that uses the same key to both encrypt and decrypt messages. DES is an example of this type of technology.
218	**System Flowchart**	A flowchart diagramming the flow of work, documents, and operations in a data processing application.
219	**System Integrity**	The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system.
220	**System Policy**	A policy used to control what a user can do and the environment of that user. System policies can be in Windows NT, applied to a specific user, group, computer, or all users. System policies work by overwriting current settings in the registry with the system policy settings.
221	**System Specification**	A baseline specification containing all the essential computer-based business system documentation. It is completed at the end of the Development Phase.
222	**Systemic Risk**	The risk that the failure of one participant in a funds transfer system, or in financial markets, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations when due.
223	**Systems Analysis**	The performance, management, and documentation of the four phases of the life cycle of a business system: study, design, development, and operation.
224	**Tamper Resistant**	The capacity of devices to resist physical attack up to a certain point.
225	**Tamper-Evident**	The capacity of devices to show evidence of physical attack.
226	**Tamper-Proof**	The proven capacity of devices to resist attacks.
227	**Telecommunications**	Data transmission between a computing system and remotely located devices by telephone lines, cable, or wireless technology.
228	**Telnet**	A protocol that permits users to access a remote terminal or another computer through a network; widely used on the Internet.
229	**Thread**	A list of instructions running in a computer to perform a certain task. Each thread runs in the context of a process, which embodies the protected memory space and the environment of the threads. Multi-threaded processes can perform more than one task at the same time.
230	**Threat Monitoring**	The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security.
231	**Throughput**	The total amount of useful work performed by a data processing system during a given period of time.
232	**Topology**	The arrangement of nodes usually forming a star, ring, tree, or bus pattern.
233	**Topology**	The arrangement of nodes usually forming a star, ring, tree, or bus pattern.
234	**Traceability**	The degree to which transactions can be traced to the originator or recipient (also referred to as auditability).
235	**Transferability**	In electronic money systems, the degree to which an electronic balance can be transferred between devices without interaction with a central authority.
236	**Transport Control Protocol/Internet Protocol (TCP/IP)**	A standard format for transmitting data in packets from one computer to another, on the Internet and within other networks. TCP deals with the construction of the data packets while IP routes them from machine to machine.
237	**Trap Door**	A concealed and unauthorized entrance into a computer operating system, designed by the programmer.

	A	B
238	**Trojan Horse**	A program that appears to perform a useful function and sometimes does so quite well but also includes an unadvertised feature, which is usually malicious in nature.
239	**Truncation**	Dropping off part of a character string either to conserve space or because of limited space.
240	**Trusted Computer System**	A system that employs sufficient assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.
241	**Trusted Relationship**	Links between domains that enable pass-through validation, in which a user has only one user account in one domain, yet can access the entire network. A trusting domain honors the log in validation of another trusted domain. A key weakness with these systems is that a hacker may try to gain access to a lesser secured system to take advantage of its trust relationship with other computers.
242	**Trusted Third Party**	A reputable entity that authenticates one or more parties to an electronic transaction. The authentication process generally involves the issuance and administration of digital certificates.
243	**Uniform Resource Locator or Universal Resource Locator (URL)**	A way of specifying the location of available information on the Internet.
244	**Uninterruptible Power Supply (UPS)**	Provides power to a system in case of a power outage.
245	**UNIX**	A multitasking, kernel-based operating system developed by AT&T in the early 1970s and provided, originally, free to universities as a research operating system. Because of its availability and ability to scale down to microprocessor-based computers, UNIX became the standard operating system of the Internet and its attendant network protocols and is the closest approximation to a universal operating system that exists. Most computers can run some variant of the UNIX operating system.
246	**Upload**	To transmit a file to a central computer from a smaller computer or a remote location.
247	**Usenet**	A set of many newsgroups distributed via the Internet.
248	**User Manager for Domains**	A tool used to manage security for a domain or an individual computer. Administers user accounts, groups, and security policies.
249	**Virtual Corporations**	Corporations that have no official physical site presence and are made up of diverse geographically dispersed or mobile employees.
250	**Virus**	A program with the ability to reproduce by modifying other programs to include a copy of itself. It may contain destructive code that can move into multiple programs, data files, or devices on a system and spread through multiple systems in a network.
251	**Vulnerability**	A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security.
252	**War-Dialing**	Dialing every number on an institution’s telephone exchange looking for the existence of authorized or unauthorized modems on which to launch an attack.
253	**Web Page**	Information presented through a Web browser in a single view.
254	**Web Site**	A Web page or set of Web pages designed, presented, and linked together to form a logical information resource and/or transaction initiation function.
255	**Wide Area Network (WAN)**	A communications network that covers a wide geographic area, such as state or country, using high speed long distance lines or satellites provided by a common carrier.
256	**Win 16**	The set of application services provided by the 16-bit versions of Windows 3.1 and Windows for Workgroups 3.11
257	**Win 32**	The set of applications services provided by the 32-bit versions of Windows 95 and NT.
258	**Windows 95**	A 32-bit version Windows for medium-range, Intel-based computers. This system includes peer networking services, Internet support, and strong support for older DOS applications and peripherals.
259	**Windows NT**	The portable, secure, 32-bit, preemptive multitasking member of the Windows operating system family. This system includes peer networking services, server networking services, Internet client and server services, and a broad range of utilities.
260	**Windows NT Server**	The Windows NT Server provides centralized management and security, advanced fault tolerance, and additional connectivity.
261	**Workgroup**	A collection of computers that are grouped for viewing purposes. Each workgroup is identified by a unique name.
262	**Workstation**	A powerful personal computer.
263	**World Wide Web (Web, WWW)**	A subnetwork of the Internet through which information is exchanged via text, graphics, audio, and video.
264	**Worm**	A program that scans a system or an entire network for available, unused space in which to run. Worms tend to tie up all computing resources in a system or on a network and effectively shut it down.