Comptroller of the Currency
Administrator of National Banks

Internet Banking

Comptroller's Handbook

October 1999

This booklet provides guidance to bankers and examiners on identifying and controlling the risks associated with Internet banking activities. It is one of a series of specialized booklets in the Comptroller's Handbook*.*

"Internet banking" refers to systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC) or other intelligent device.

Internet banking products and services can include wholesale products for corporate customers as well as retail and fiduciary products for consumers. Ultimately, the products and services obtained through Internet banking may mirror products and services offered through other bank delivery channels. Some examples of wholesale products and services include:

- Cash management.
- Wire transfer.
- Automated clearinghouse (ACH) transactions.
- Bill presentment and payment.

Examples of retail and fiduciary products and services include:

- Balance inquiry.
- Funds transfer.
- Downloading transaction information.
- Bill presentment and payment.
- Loan applications.
- Investment activity.
- Other value-added services.

Other Internet banking services may include providing Internet access as an Internet Service Provider (ISP). The OCC has determined that a national bank subsidiary may provide home banking services through an Internet connection to the bank's home banking system and, incidental to that service, may also provide Internet access to bank customers using that service (see OCC Interpretive Letter No. 742, the "Apollo" letter). Historically, banks have used information systems technology to process checks (item processing), drive ATM machines (transaction processing), and produce reports (management

information systems). In the past, the computer systems that made the information systems operate were rarely noticed by customers. Today, Web sites, electronic mail, and electronic bill presentment and payment systems are an important way for banks to reach their customers.

National banks have experimented with various forms of online banking for many years. Some of the early experiments involved closed systems where the customers accessed banks through a dial-in or cable TV connection. These systems limited a bank's potential customer base because they required out-of-area customers to either incur long-distance charges on their phone bills or subscribe to a particular cable TV service to access the bank. With the widespread growth of the Internet, customers can use this technology anywhere in the world to access a bank's network. The Internet, as an enabling technology, has made banking products and services available to more customers and eliminated geographic and proprietary systems barriers. With an expanded market, banks also may have opportunities to expand or change their product and service offerings.

Growth in Internet Banking

Numerous factors — including competitive cost, customer service, and demographic considerations — are motivating banks to evaluate their technology and assess their electronic commerce and Internet banking strategies. Many researchers expect rapid growth in customers using online banking products and services. The challenge for national banks is to make sure the savings from Internet banking technology more than offset the costs and risks associated with conducting business in cyberspace.

Marketing strategies will vary as national banks seek to expand their markets and employ lower cost delivery channels. Examiners will need to understand the strategies used and technologies employed on a bank-by-bank basis to assess the risk. Evaluating a bank's data on the use of their Web sites, may help examiners determine the bank's strategic objectives, how well the bank is meeting its Internet banking product plan, and whether the business is expected to be profitable.

Some of the market factors that may drive a bank's strategy include the following:

Competition — Studies show that competitive pressure is the chief driving force behind increasing use of Internet banking technology, ranking ahead of cost reduction and revenue enhancement, in second and third place respectively. Banks see Internet banking as a way to keep existing customers and attract new ones to the bank.

Cost Efficiencies — National banks can deliver banking services on the Internet at transaction costs far lower than traditional brick-and-mortar branches. The actual costs to execute a transaction will vary depending on the delivery channel used. For example, according to Booz, Allen & Hamilton, as of mid-1999, the cost to deliver manual transactions at a branch was typically more than a dollar, ATM and call center transactions cost about 25 cents, and Internet transactions cost about a penny. These costs are expected to continue to decline.

National banks have significant reasons to develop the technologies that will help them deliver banking products and services by the most cost-effective channels. Many bankers believe that shifting only a small portion of the estimated 19-billion payments mailed annually in the U.S. to electronic delivery channels could save banks and other businesses substantial sums of money. However, national banks should use care in making product decisions. Management should include in their decision making the development and ongoing costs associated with a new product or service, including the technology, marketing, maintenance, and customer support functions. This will help management exercise due diligence, make more informed decisions, and measure the success of their business venture.

Geographical Reach — Internet banking allows expanded customer contact through increased geographical reach and lower cost delivery channels. In fact some banks are doing business exclusively via the Internet — they do not have traditional banking offices and only reach their customers online. Other financial institutions are using the Internet as an alternative delivery channel to reach existing customers and attract new customers.

Branding — Relationship building is a strategic priority for many national banks. Internet banking technology and products can provide a means for national banks to develop and maintain an ongoing relationship with their customers by offering easy access to a broad array of products and services.

By capitalizing on brand identification and by providing a broad array of financial services, banks hope to build customer loyalty, cross-sell, and enhance repeat business.

Customer Demographics — Internet banking allows national banks to offer a wide array of options to their banking customers. Some customers will rely on traditional branches to conduct their banking business. For many, this is the most comfortable way for them to transact their banking business. Those customers place a premium on person-to-person contact. Other customers are early adopters of new technologies that arrive in the marketplace. These customers were the first to obtain PCs and the first to employ them in conducting their banking business. The demographics of banking customers will continue to change. The challenge to national banks is to understand their customer base and find the right mix of delivery channels to deliver products and services profitably to their various market segments.

Types of Internet Banking

Understanding the various types of Internet banking products will help examiners assess the risks involved. Currently, the following three basic kinds of Internet banking are being employed in the marketplace:

- Informational — This is the basic level of Internet banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server. The risk is relatively low, as informational systems typically have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or outsourced. While the risk to a bank is relatively low, the server or Web site may be vulnerable to alteration. Appropriate controls therefore must be in place to prevent unauthorized alterations to the bank's server or Web site.

- Communicative — This type of Internet banking system allows some interaction between the bank's systems and the customer. The interaction may be limited to electronic mail, account inquiry, loan applications, or static file updates (name and address changes). Because these servers may have a path to the bank's internal networks, the risk is higher with this configuration than with informational systems. Appropriate controls need to be in place to prevent, monitor, and alert management of any unauthorized attempt to access the bank's internal

networks and computer systems. Virus controls also become much more critical in this environment.

- Transactional — This level of Internet banking allows customers to execute transactions. Since a path typically exists between the server and the bank's or outsourcer's internal network, this is the highest risk architecture and must have the strongest controls. Customer transactions can include accessing accounts, paying bills, transferring funds, etc.

Internet Banking Risks

Internet banking creates new risk control challenges for national banks. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital. The OCC has defined nine categories of risk for bank supervision purposes. The risks are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic, and reputation. These categories are not mutually exclusive and all of these risks are associated with Internet banking.

Credit Risk

Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed. Credit risk is found in all activities where success depends on counterparty, issuer, or borrower performance. It arises any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether on or off the banks balance sheet.

Internet banking provides the opportunity for banks to expand their geographic range. Customers can reach a given institution from literally anywhere in the world. In dealing with customers over the Internet, absent any personal contact, it is challenging for institutions to verify the bonafides of their customers, which is an important element in making sound credit decisions. Verifying collateral and perfecting security agreements also can be challenging with out-of-area borrowers. Unless properly managed, Internet banking could lead to a concentration in out-of-area credits or credits within a single industry. Moreover, the question of which state's or country's laws control an Internet relationship is still developing.

Effective management of a portfolio of loans obtained through the Internet requires that the board and management understand and control the bank's lending risk profile and credit culture. They must assure that effective policies, processes, and practices are in place to control the risk associated with such loans. *See* the "Loan Portfolio Management," booklet of the *Comptroller's Handbook* for a more complete discussion of credit risk.

Interest Rate Risk

Interest rate risk is the risk to earnings or capital arising from movements in interest rates. From an economic perspective, a bank focuses on the sensitivity of the value of its assets, liabilities and revenues to changes in interest rates. Interest rate risk arises from differences between the timing of rate changes and the timing of cash flows (repricing risk); from changing rate relationships among different yield curves affecting bank activities (basis risk); from changing rate relationships across the spectrum of maturities (yield curve risk); and from interest-related options embedded in bank products (options risk). Evaluation of interest rate risk must consider the impact of complex, illiquid hedging strategies or products, and also the potential impact that changes in interest rates will have on fee income. In those situations where trading is separately managed, this refers to structural positions and not trading portfolios.

Internet banking can attract deposits, loans, and other relationships from a larger pool of possible customers than other forms of marketing. Greater access to customers who primarily seek the best rate or term reinforces the need for managers to maintain appropriate asset/liability management systems, including the ability to react quickly to changing market conditions.

Liquidity Risk

Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned changes in funding sources. Liquidity risk also arises from the failure to recognize or address changes in market conditions affecting the ability of the bank to liquidate assets quickly and with minimal loss in value.

Internet banking can increase deposit volatility from customers who maintain accounts solely on the basis of rate or terms. Asset/liability and loan portfolio management systems should be appropriate for products offered through

Internet banking. Increased monitoring of liquidity and changes in deposits and loans may be warranted depending on the volume and nature of Internet account activities.

Price Risk

Price risk is the risk to earnings or capital arising from changes in the value of traded portfolios of financial instruments. This risk arises from market making, dealing, and position taking in interest rate, foreign exchange, equity, and commodities markets.

Banks may be exposed to price risk if they create or expand deposit brokering, loan sales, or securitization programs as a result of Internet banking activities. Appropriate management systems should be maintained to monitor, measure, and manage price risk if assets are actively traded.

Foreign Exchange Risk

Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency. In some cases, banks will enter into multi-currency credit commitments that permit borrowers to select the currency they prefer to use in each rollover period. Foreign exchange risk can be intensified by political, social, or economic developments. The consequences can be unfavorable if one of the currencies involved becomes subject to stringent exchange controls or is subject to wide exchange-rate fluctuations. Foreign exchange risk is discussed in more detail in the "Foreign Exchange," booklet of the *Comptroller's Handbook*.

Banks may be exposed to foreign exchange risk if they accept deposits from non-U.S. residents or create accounts denominated in currencies other than U.S. dollars. Appropriate systems should be developed if banks engage in these activities.

Transaction Risk

Transaction risk is the current and prospective risk to earnings and capital arising from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information. Transaction risk is evident in each product and service offered and encompasses product

development and delivery, transaction processing, systems development, computing systems, complexity of products and services, and the internal control environment.

A high level of transaction risk may exist with Internet banking products, particularly if those lines of business are not adequately planned, implemented, and monitored. Banks that offer financial products and services through the Internet must be able to meet their customers' expectations. Banks must also ensure they have the right product mix and capacity to deliver accurate, timely, and reliable services to develop a high level of confidence in their brand name. Customers who do business over the Internet are likely to have little tolerance for errors or omissions from financial institutions that do not have sophisticated internal controls to manage their Internet banking business. Likewise, customers will expect continuous availability of the product and Web pages that are easy to navigate.

Software to support various Internet banking functions is provided to the customer from a variety of sources. Banks may support customers using customer-acquired or bank-supplied browsers or personal financial manager (PFM) software. Good communications between banks and their customers will help manage expectations on the compatibility of various PFM software products.

Attacks or intrusion attempts on banks' computer and network systems are a major concern. Studies show that systems are more vulnerable to internal attacks than external, because internal system users have knowledge of the system and access. Banks should have sound preventive and detective controls to protect their Internet banking systems from exploitation both internally and externally. *See* OCC Bulletin 99-9, "Infrastructure Threats from Cyber-Terrorists" for additional information.

Contingency and business resumption planning is necessary for banks to be sure that they can deliver products and services in the event of adverse circumstances. Internet banking products connected to a robust network may actually make this easier because back up capabilities can be spread over a wide geographic area. For example, if the main server is inoperable, the network could automatically reroute traffic to a back up server in a different geographical location. Security issues should be considered when the institution develops its contingency and business resumption plans. In such situations, security and internal controls at the back-up location should be as

sophisticated as those at the primary processing site. High levels of system availability will be a key expectation of customers and will likely differentiate success levels among financial institutions on the Internet.

National banks that offer bill presentment and payment will need a process to settle transactions between the bank, its customers, and external parties. In addition to transaction risk, settlement failures could adversely affect reputation, liquidity, and credit risk.

Compliance Risk

Compliance risk is the risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested. Compliance risk exposes the institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and lack of contract enforceability.

Most Internet banking customers will continue to use other bank delivery channels. Accordingly, national banks will need to make certain that their disclosures on Internet banking channels, including Web sites, remain synchronized with other delivery channels to ensure the delivery of a consistent and accurate message to customers.

Federal consumer protection laws and regulations, including CRA and Fair Lending, are applicable to electronic financial services operations including Internet banking. Moreover, it is important for national banks to be familiar with the regulations that permit electronic delivery of disclosures/notices versus those that require traditional hard copy notification. National banks should carefully review and monitor all requirements applicable to electronic products and services and ensure they comply with evolving statutory and regulatory requirements.

Advertising and record-keeping requirements also apply to banks' Web sites and to the products and services offered. Advertisements should clearly and conspicuously display the FDIC insurance notice, where applicable, so customers can readily determine whether a product or service is insured.

Regular monitoring of bank Web sites will help ensure compliance with applicable laws, rules, and regulations. *See* the "Consumer Compliance Examination" booklet of the *Comptroller's Handbook*, OCC Bulletin 94-13, "Nondeposit Investment Sales Examination Procedures," and OCC Bulletin 98-31, "Guidance on Electronic Financial Services and Consumer Compliance" for more information.

Application of Bank Secrecy Act (BSA) requirements to cyberbanking products and services is critical. The anonymity of banking over the Internet poses a challenge in adhering to BSA standards. Banks planning to allow the establishment of new accounts over the Internet should have rigorous account opening standards. Also, the bank should set up a control system to identify unusual or suspicious activities and, when appropriate, file suspicious activity reports (SARs).

The BSA funds transfer rules also apply to funds transfers or transmittals performed over the Internet when transactions exceed $3,000 and do not meet one of the exceptions. The rules require banks to ensure that customers provide all the required information before accepting transfer instructions. The record keeping requirements imposed by the rules allow banks to retain written or electronic records of the information.

The Office of Foreign Asset Control (OFAC) administers laws that impose economic sanctions against foreign nations and individuals. This includes blocking accounts and other assets and prohibiting financial transactions. Internet banking businesses must comply with OFAC requirements. A bank needs to collect enough information to identify customers and determine whether a particular transaction is prohibited under OFAC rules. *See* the *FFIEC Information Systems Examination Handbook* (*IS Handbook*) for a discussion of OFAC.

Strategic Risk

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication

channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

Management must understand the risks associated with Internet banking before they make a decision to develop a particular class of business. In some cases, banks may offer new products and services via the Internet. It is important that management understand the risks and ramifications of these decisions. Sufficient levels of technology and MIS are necessary to support such a business venture. Because many banks will compete with financial institutions beyond their existing trade area, those engaging in Internet banking must have a strong link between the technology employed and the bank's strategic planning process.

Before introducing a Internet banking product, management should consider whether the product and technology are consistent with tangible business objectives in the bank's strategic plan. The bank also should consider whether adequate expertise and resources are available to identify, monitor, and control risk in the Internet banking business. The planning and decision making process should focus on how a specific business need is met by the Internet banking product, rather than focusing on the product as an independent objective. The bank's technology experts, along with its marketing and operational executives, should contribute to the decision making and planning process. They should ensure that the plan is consistent with the overall business objectives of the bank and is within the bank's risk tolerance. New technologies, especially the Internet, could bring about rapid changes in competitive forces. Accordingly, the strategic vision should determine the way the Internet banking product line is designed, implemented, and monitored.

Reputation Risk

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the institution to litigation, financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with customers and the community.

A bank's reputation can suffer if it fails to deliver on marketing claims or to provide accurate, timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to customer inquiries, or violations of customer privacy expectations.

A bank's reputation can be damaged by Internet banking services that are poorly executed or otherwise alienate customers and the public. Well designed marketing, including disclosures, is one way to educate potential customers and help limit reputation risk. Customers must understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using the system. As such, marketing concepts need to be coordinated closely with adequate disclosure statements. A national bank should not market the bank's Internet banking system based on features or attributes the system does not have. The marketing program must present the product fairly and accurately.

National banks should carefully consider how connections to third parties are presented on their Web sites. Hypertext links are often used to enable a customer to link to a third party. Such links may reflect an endorsement of the third party's products or services in the eyes of the customer. It should be clear to the customer when they have left the bank's Web site so that there is no confusion about the provider of the specific products and services offered or the security and privacy standards that apply. Similarly, adequate disclosures must be made so that customers can distinguish between insured and non-insured products.

National banks need to be sure that their business continuity plans include the Internet banking business. Regular testing of the business continuity plan, including communications strategies with the press and public, will help the bank ensure it can respond effectively and promptly to any adverse customer or media reactions.

Risk Management

Financial institutions should have a technology risk management process to enable them to identify, measure, monitor, and control their technology risk exposure. Examiners should refer to OCC Bulletin 98-3, "Technology Risk Management" for additional guidance on this topic. Risk management of new technologies has three essential elements:

- The planning process for the use of the technology.
- Implementation of the technology.
- The means to measure and monitor risk.

The OCC's objective is to determine whether a bank is operating its Internet banking business in a safe and sound manner. The OCC expects banks to use a rigorous analytic process to identify, measure, monitor, and control risk. Examiners will determine whether the level of risk is consistent with the bank's overall risk tolerance and is within the bank's ability to manage and control.

The risk planning process is the responsibility of the board and senior management. They need to possess the knowledge and skills to manage the bank's use of Internet banking technology and technology-related risks. The board should review, approve, and monitor Internet banking technology-related projects that may have a significant impact on the bank's risk profile. They should determine whether the technology and products are in line with the bank's strategic goals and meet a need in their market. Senior management should have the skills to evaluate the technology employed and risks assumed. Periodic independent evaluations of the Internet banking technology and products by auditors or consultants can help the board and senior management fulfill their responsibilities.

Implementing the technology is the responsibility of management. Management should have the skills to effectively evaluate Internet banking technologies and products, select the right mix for the bank, and see that they are installed appropriately. If the bank does not have the expertise to fulfill this responsibility internally, it should consider contracting with a vendor who specializes in this type of business or engaging in an alliance with another provider with complementary technologies or expertise.

Measuring and monitoring risk is the responsibility of management. Management should have the skills to effectively identify, measure, monitor, and control risks associated with Internet banking. The board should receive regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. As part of the design process, a national bank should include effective quality assurance and audit processes in its Internet banking system. The bank

should periodically review the systems to determine whether they are meeting the performance standards.

Internal Controls

Internal controls over Internet banking systems should be commensurate with an institution's level of risk. As in any other banking area, management has the ultimate responsibility for developing and implementing a sound system of internal controls over the bank's Internet banking technology and products.

Regular audits of the control systems will help ensure that the controls are appropriate and functioning properly. For example, the control objectives for an individual bank's Internet banking technology and products might focus on:

- Consistency of technology planning and strategic goals, including efficiency and economy of operations and compliance with corporate policies and legal requirements.
- Data availability, including business recovery planning.
- Data integrity, including providing for the safeguarding of assets, proper authorization of transactions, and reliability of the process and output.
- Data confidentiality and privacy safeguards.
- Reliability of MIS.

Once control objectives are established, management has the responsibility to install the necessary internal controls to see that the objectives are met. Management also has the responsibility to evaluate the appropriateness of the controls on a cost-benefit basis. That analysis may take into account the effectiveness of each control in a process, the dollar volume flowing through the process, and the cost of the controls.

Examiners will need to understand the bank's operational environment to evaluate the proper mix of internal controls and their adequacy. According to the Information Systems Audit and Control Association (ISACA) the basic internal control components include:

- Internal accounting controls — Used to safeguard the assets and reliability of financial records. These would include transaction records and trial balances

- Operational controls — Used to ensure that business objectives are being met. These would include operating plans and budgets to compare actual against planned performance.
- Administrative controls — Used to ensure operational efficiency and adherence to policies and procedures. These would include periodic internal and external audits.

ISACA separates internal controls into three general categories. The three control categories can be found in the basic internal controls discussed above.

- Preventive Controls — Prevent something (often an error or illegal act) from happening. An example of this type of control is logical access control software that would allow only authorized persons to access a network using a combination of a user ID and password.

- Detective Controls — Identify an action that has occurred. An example would be intrusion detection software that triggers an alert or alarm.

- Corrective Controls — Correct a situation once it has been detected. An example would be software backups that could be used to recover a corrupted file or database.

Banks or service providers offering transaction-based Internet banking products need to have a high level of controls to help manage the bank's transaction risk. Examples of these controls could include:

- Monitoring transaction activity to look for anomalies in transaction types, transaction volumes, transaction values, and time-of-day presentment.

- Monitoring log-on violations or attempts to identify patterns of suspect activity including unusual requests, unusual timing, or unusual formats.

- Using trap and trace techniques to identify the source of the request and match these against known customers.

Regular reporting and review of unusual transactions will help identify:

- Intrusions by unauthorized parties.
- Customer input errors.
- Opportunities for customer education.

Technology: In-House or Outsourced?

The different levels of complexity associated with certain areas involving security, operations, planning, and monitoring have caused many national banks to outsource all or parts of their Internet banking operations. Banks should periodically reassess their sources of technology support to determine whether a given solution continues to fit their business plan and is flexible enough to meet anticipated future needs. Regardless of whether technology services are provided in-house or through a third-party servicer, national banks need to have a strong link between their technology provider and their strategic planning process. This will enable the bank to link new products and services with the existing technology and product mix.

There are pros and cons to offering technology-based products and services in-house versus contracting with a vendor. Larger national banks with substantial resources may choose to purchase computer hardware and operating systems and/or develop the necessary application software in-house. This option may provide the greatest flexibility to customize product offerings.

Other banks may choose to purchase a "turnkey" system from a vendor. In this arrangement the vendor typically provides the hardware, operating systems, and applications software necessary to enable the bank to offer the particular product or service to its customers. The vendor will typically provide the service and maintenance for the turnkey system. A variation is to outsource the service. Using this option, national banks contract with a vendor to operate their Internet banking Web sites at the vendor's location. This option may be especially well suited for banks that do not have the technical expertise to develop this service in-house. However, such banks need to place additional emphasis on their due diligence to ensure that security is not compromised.

Several companies are responding to the developing markets for Web pages, Internet banking applications, and bill presentment and payment services.

Although many companies in this market are prosperous and well managed, some are start-up companies with unproven products, services, or track records.

National banks need to perform due diligence before selecting a vendor to provide Internet banking services. They should have a formal service agreement with the vendor that clearly addresses the duties and responsibilities of the parties involved. National banks need to monitor their vendor's operational performance, financial condition, and capability to stay current with evolving technologies. National banks typically fulfill their responsibility to assure their vendors have sound internal controls by obtaining internal or third-party audit reports.

Examiners should refer to the *IS Handbook* for a complete discussion of outsourcing issues. Whatever the source of Internet banking technology, products, and services, it is important for the national bank to have personnel with an appropriate level of specialized expertise, consistent with risk, to monitor and manage the business.

Issues in Internet Banking

Financial institutions, their card associations, and vendors are working to develop an Internet payment infrastructure to help make electronic commerce secure. Many in the banking industry expect significant growth in the use of the Internet for the purchase of goods and services and electronic data interchange. The banking industry also recognizes that the Internet must be secure to achieve a high level of confidence with both consumers and businesses.

Sound management of banking products and services, especially those provided over the Internet, is fundamental to maintaining a high level of public confidence not only in the individual bank and its brand name but also in the banking system as a whole. Key components that will help maintain a high level of public confidence in an open network environment include:

- Security
- Authentication
- Trust
- Nonrepudiation
- Privacy

C Availability

Security is an issue in Internet banking systems. The OCC expects national banks to provide a level of logical and physical security commensurate with the sensitivity of the information and the individual bank's risk tolerance.

Some national banks allow for direct dial-in access to their systems over a private network while others provide network access through the Internet. Although the publicly accessible Internet generally may be less secure, both types of connections are vulnerable to interception and alteration. For example, hardware or software "sniffers" can obtain passwords, account numbers, credit card numbers, etc. without regard to the means of access. National banks therefore must have a sound system of internal controls to protect against security breaches for all forms of electronic access. A sound system of preventive, detective, and corrective controls will help assure the integrity of the network and the information it handles. See appendix C for a discussion of online attacks.

Firewalls are frequently used on Internet banking systems as a security measure to protect internal systems and should be considered for any system connected to an outside network. Firewalls are a combination of hardware and software placed between two networks through which all traffic must pass, regardless of the direction of flow. They provide a gateway to guard against unauthorized individuals gaining access to the bank's network.

The mere presence of a firewall does not assure logical security and firewalls are not impenetrable: firewalls must be configured to meet a specific operating environment and they must be evaluated and maintained on a regular basis to assure their effectiveness and efficiency. Individuals who are technically competent must perform the installation, configuration, evaluation, and maintenance of firewalls. The specific risks involved may require a broad range of security controls. Appendix A contains a more detailed discussion of firewalls and associated controls.

The *IS Handbook* discusses other logical and physical security controls applicable to Internet banking environments. Examiners should be familiar with these controls before conducting a Internet banking examination.

Authentication is another issue in a Internet banking system. Transactions on the Internet or any other telecommunication network must be secure to achieve

a high level of public confidence. In cyberspace, as in the physical world, customers, banks, and merchants need assurances that they will receive the service as ordered or the merchandise as requested, and that they know the identity of the person they are dealing with.

Banks typically use symmetric (private key) encryption technology to secure messages and asymmetric (public/private key) cryptography to authenticate parties. Asymmetric cryptography employs two keys — a public key and a private key. These two keys are mathematically tied but one key cannot be deduced from the other. For example, to authenticate that a message came from the sender, the sender encrypts the message using their private key. Only the sender knows the private key. But, once sent, the message can be read only using the sender's public key. Since the message can only be read using the sender's public key, the receiver knows the message came from the expected sender.

Internet banking systems should employ a level of encryption that is appropriate to the level or risk present in the systems. OCC is aware that stronger levels of encryption may slow or degrade performance and, accordingly, management must balance security needs with performance and cost issues. Thus, a national bank should conduct a risk assessment in deciding upon its appropriate level of encryption. The OCC does not mandate a particular strength or type of encryption. Rather, it expects management to evaluate security risks, review the cost and benefit of different encryption systems, and decide on an appropriate level of encryption as a business decision. Management should be able to explain the supporting analysis for their decision.

A common asymmetric cryptography system is RSA, which uses key lengths up to 1,024 bits. By using the two forms of cryptography together, symmetric to protect the message and asymmetric to authenticate the parties involved, banks can secure the message and have a high level of confidence in the identity of the parties involved. See appendix B of this handbook for examples of how this technology works.

Biometric devices are an advanced form of authentication. These devices may take the form of a retina scan, finger or thumb print scan, facial scan, or voice print scan. Use of biometrics is not yet considered mainstream, but may be used by some banks for authentication. Examiners should evaluate biometric

activities based on management's understanding of risks, internal or external reviews, and the overall performance of these devices.

Trust is another issue in Internet banking systems. As noted in the previous discussion, public and private key cryptographic systems can be used to secure information and authenticate parties in transactions in cyberspace. A trusted third party is a necessary part of the process. That third party is the *certificate authority*.

A certificate authority is a trusted third party that verifies identities in cyberspace. Some people think of the certificate authority functioning like an online notary. The basic concept is that a bank, or other third party, uses its good name to validate parties in transactions. This is similar to the historic role banks have played with letters of credit, where neither the buyer nor seller knew each other but both parties were known to the bank. Thus the bank uses its good name to facilitate the transaction, for a fee. *See* OCC Bulletin 99-20, "Certification Authority Services," for more information on this topic.

Banks also may need a way to validate themselves in cyberspace, as theft of identity has taken place. According to GAO testimony (GAO/T-66D-99-34), perpetrators have copied legitimate brokerage-firm Web sites, altered addresses for customers to contact (and send checks), then put the fraudulent Web site back on the Internet. Except for the post office box and possibly the URL, everything on the Web site could appear legitimate. Banks will have to guard against a variety of frauds and scams as banking on the Internet becomes more prominent. A proper mix of preventive, detective, and corrective controls can help protect national banks from these pitfalls. Digital certificates may play an important role in authenticating parties and thus establishing trust in Internet banking systems.

Nonrepudiation is the undeniable proof of participation by both the sender and receiver in a transaction. It is the reason public key encryption was developed, i.e., to authenticate electronic messages and prevent denial or repudiation by the sender or receiver.

Although technology has provided an answer to nonrepudiation, state laws are not uniform in the treatment of electronic authentication and digital signatures. The application of state laws to these activities is a new and emerging area of the law.

Privacy is a consumer issue of increasing importance. National banks that recognize and respond to privacy issues in a proactive way make this a positive attribute for the bank and a benefit for its customers.

Public concerns over the proper versus improper accumulation and use of personal information are likely to increase with the continued growth of electronic commerce and the Internet. Providers who are sensitive to these concerns have an advantage over those who do not. *See* OCC Advisory Letter 99-6, "Guidance to National Banks on Web Site Privacy Statements," for a more complete discussion of this topic.

Availability is another component in maintaining a high level of public confidence in a network environment. All of the previous components are of little value if the network is not available and convenient to customers. Users of a network expect access to systems 24 hours per day, seven days a week.

Among the considerations associated with system availability are capacity, performance monitoring, redundance, and business resumption. National banks and their vendors who provide Internet banking products and services need to make certain they have the capacity in terms of hardware and software to consistently deliver a high level of service.

In addition, performance monitoring techniques will provide management with information such as the volume of traffic, the duration of transactions, and the amount of time customers must wait for service. Monitoring capacity, downtime, and performance on a regular basis will help management assure a high level of availability for their Internet banking system.

It is also important to evaluate network vulnerabilities to prevent outages due to component failures. An entire network can become inoperable when a single hardware component or software module malfunctions. Often national banks and their vendors will employ redundant hardware in critical areas or have the ability to switch to alternate processing locations. The latter is often referred to as contingency planning. This topic is covered at length in the *IS Handbook*.

In addition to these issues, appendix D contains some discussion points examiners can use in national banks that are contemplating engaging in Internet banking.

General Procedures

The objective of these examination procedures is to determine the adequacy of the institution's policies, procedures, and internal controls as they relate to Internet banking. The extent of testing and procedures performed should be based upon the examiner's assessment of risk. This assessment should include consideration of work performed by internal and external auditors, formal policies and procedures, and the effectiveness of internal controls and management information systems (MIS).

Examiners should use the *FFIEC Information Systems Examination Handbook* and related OCC issuances for additional information and guidance as referenced in these procedures.

It may not be necessary to complete all the procedures. When planning, examiners should determine the extent of the bank's reliance on external vendors for Internet banking operations and/or monitoring activities. Procedures to evaluate outsourced activities are incorporated in these general procedures.

Objective: To set the scope for assessing the quantity of risk and quality of risk management in Internet banking.

1. Review the following documents to identify any previously noted problems related to the Internet banking area that require follow-up:

   - Previous examination reports (Asset Management, BIS, Commercial, Compliance, etc.).
   - Supervisory strategy.
   - EIC scope memorandum.
   - Follow-up activities.
   - Work papers from previous examinations.
   - Internal and external audit reports.

- Correspondence.

(Note: If an examiner is assigned Internal and External Audit, a copy of any significant deficiencies for this area should be obtained from that examiner. If internal and external audit is not part of the overall scope of the examination, review the work performed by the internal and external auditors in this area and obtain a list of any deficiencies noted in their most recent review.)

2. Verify the completeness of requested information with the request list.

3. Obtain other reviews, assessments or system certifications performed by internal/external auditors, consultants, or technology experts contracted by the bank. Note any outstanding deficiencies.

4. Determine whether external vendors are used and what services or products are provided. Examiners should document the major entities responsible for development, operation, and/or support of all or portions of Internet banking systems.

5. Review documentation and conduct early discussions with management to determine:

   (Note: Consultation with examiners responsible for reviewing overall bank information security should be performed and work papers reviewed to avoid any redundancy in reviewing security controls.)

   - How security for Internet banking is addressed.
   - How management supervises Internet banking functions, including those functions that are outsourced.
   - Any significant changes in policies, practices, personnel, or control systems.
   - Any internal or external factors that could affect the Internet banking area.

6. Review the bank's business and strategic plans to determine whether management's plans for the Internet banking business are clear and reflect the current direction of the unit.

7. Determine whether management has incorporated Internet banking as part of contingency and business resumption plans.

8. Gain an understanding of the bank's Internet banking business and disclosures by reviewing the bank's Web site(s).

9. Based on the performance of the previous steps, combined with discussions with the EIC and other appropriate supervisors and examiners, determine the scope and objectives of this examination.

10. As examination procedures are performed, test for compliance with established policies or practices and the existence of appropriate internal control processes. Identify any area with inadequate supervision and/or undue risk, and discuss with the EIC the need to perform additional procedures.

Select from among the following examination procedures the steps that are necessary to meet examination objectives. An examination will seldom require every step to be performed.

Quantity of Risk

Conclusion: The quantity of risk is (low, moderate, high).

Internet Banking Products and Services

Objective: To gain an understanding of the type and volume of the bank's Internet banking product line, transaction flow and settlement processes.

1. Obtain a description or diagram of the configuration of the Internet banking system and its capabilities. Consider hardware, software, points of connectivity to internal systems, and remote access points. To help determine the level of risk, evaluate:

   - How the Internet banking system is linked to other host systems or the network infrastructure in the bank.
   - How transactions and data flow through the network.
   - What type(s) of telecommunications channels and remote access capabilities (direct modem dial-in, Internet access, or both) exist.

2. Identify the current types, volumes, and complexity of retail, wholesale, and fiduciary products and services in the bank's Internet banking product and services line.

3. Review systems and network architecture to identify access points and potential areas of vulnerability.

4. Through discussion with management, note any changes in the type, volume or complexity of products or services expected in the next two years.

5. Evaluate Internet banking marketing strategies to determine whether plans include expansion into new markets, product lines, or other technologies.

6. Obtain from management an overview of transaction and payment services flow and settlement processes and determine whether:

   - Management understands the transaction flow and settlement processes between the parties involved.
   - The bank's settlement responsibilities are clearly defined.
   - Based on the settlement process, the bank assumes additional credit risk caused by settlement time frames.
   - The vendor's policies address uncollected funds, settlement, backup, contingency, customer service, and disaster recovery.
   - There is adequate exception reporting.

7. Review the transaction and payment services products and determine whether adequate control features are built into the systems to ensure authentication of the user, data integrity, and confidentiality of transactions.

8. Determine the extent of the company's use of an Automated Clearing House (ACH) for the Internet banking products and determine whether the bank has adequate ACH controls. (See the *FFIEC Information Systems Examination Handbook* for guidance.)

9. Identify key MIS reports provided and whether they are adequate to properly manage Internet banking transaction and payment services activities.

10. Determine whether a risk assessment or audit has been performed on any vendors supporting the transaction or payment services businesses.

Compliance with Laws, Rules, and Regulations

Objective: To assess the bank's compliance with applicable banking laws.

1. Determine whether the bank is subject to notification requirements outlined in the Bank Service Corporation Act, section 1867(c)(2). (An example may include banks with investment in or partnerships with Internet service providers).

2. Identify whether the bank is staying informed on legal developments associated with Internet banking.

3. Review the findings from the most recent examinations (asset management, BIS, commercial, compliance, etc.) and the internal/external audit for issues associated with the institution's Internet banking products and services. If applicable, determine whether management has corrected any identified deficiencies.

4. Determine whether the FDIC notice is appropriately displayed and whether uninsured products or services are clearly designated (12 CFR 328).

5. Note whether reporting is in place to identify potential money laundering activities associated with Internet banking businesses.

6. Determine whether Office of Foreign Asset Control (OFAC) identification and reporting capabilities are maintained for Internet banking products and services.

7. As a way to expedite possible litigation and investigation resulting from security breaches, determine whether management has established a warning banner for users, announcing that intruders are accessing a private computer and that unauthorized access or use is not permitted and constitutes a crime punishable by law (18 USC 1030).

8. If the bank is aware of computer-related crimes *(see* AL 97-9, "Reporting Computer-Related Crimes," for guidance), determine whether a suspicious activity report was filed.

9. Determine whether the bank is providing accurate privacy disclosures associated with its Internet banking product line.

Quality of Risk Management

Conclusion: The quality of risk management is (weak, acceptable, or strong).

Policy and Strategic Planning

Objective: Determine whether the board of directors has adopted effective policies for Internet banking that are consistent with safe and sound banking practices and are appropriate to the size of the bank and the nature and scope of its operations.

1. Determine whether Internet banking security policies include:

   - Clear lines of responsibility for system security:
     - Review the duties of the security administrator and determine whether they are knowledgeable of internal security policies and controls.
     - Determine whether their authority as security administrator is adequate to dictate controls and enforce policies.
   - Network and data access control.

2. Determine whether Internet banking firewall policies address:

   - Responsibility for firewall maintenance and monitoring.
   - Well-defined access rules.
   - Access rules that dictate what traffic is allowed or forbidden.

3. Determine whether encryption is adequately addressed in the security policy, noting whether the policy includes:

   - Who is responsible for control of encryption processes.
   - How encryption is used.

   - Data classification techniques.

- Use of encryption to protect transmission of passwords, messages, or data during internal and open network communications sessions.

4. If a public key cryptographic system is used, determine whether private keys are under the control of the bank and determine whether policies and controls have been established that address private key management. Note whether policies or procedures address the following points:

   - Management of keys generated by the bank or a third party.
   - Security of secret or private key storage.
   - Who has access to the keys and how the environment is controlled.
   - If private key escrow arrangements exist, how they are controlled.
   - Procedures and practices for proper revocation and reissuance of lost, compromised, or expired keys.
   - Storage of keys on a server or computer that have no connection to outside networks.

5. Determine whether policies establish the use of virus detection software and note the products used.

6. Identify whether security policies are periodically reviewed and updated and note whether the board of directors or senior management committee approves the policies.

7. Determine whether the institution has established policies over hypertext links that enable consumers to clearly distinguish:

   - Insured and non-insured financial products.
   - Bank versus non-bank products.
   - When leaving the bank's Web site.

Processes

Objective: Determine whether processes and practices, including internal controls, are effective.

1. Evaluate the bank's short and long term strategies for Internet banking products and services through discussion with management and review of technology plans. Consider the following in assessing the bank's planning process:

   - Whether Internet banking is consistent with the bank's overall mission, strategic goals, and operating plans.
   - The level of oversight provided by the board of directors and senior management.
   - Management's understanding of industry standards to ensure compatibility and interoperability of systems.
   - Whether cost and benefit analyses of Internet banking activities consider start-up, operating, upgrade, customer support, and maintenance costs.
   - Management's evaluation of security risks, threats, and vulnerabilities.
   - The institution's internal expertise and technical training requirements.
   - The status of Y2K compliance issues as they relate to Internet banking systems.
   - Management's attention to system security monitoring and testing and performance monitoring.
   - Management's knowledge of and adherence to federal and state laws, regulations, and interpretations as they pertain to Internet banking technology and electronic commerce.

2. Determine whether management has an adequate process to periodically evaluate its Internet banking product mix and marketing successes, and links those findings to its strategic planning process.

3. Evaluate the adequacy of the bank's process for performing security risk assessments including whether it:

- Identifies threats and vulnerabilities associated with Internet banking.
- Identifies critical applications or data.
- Defines required security controls.
- Considers internal expertise and the need for external consultation or support.

4. Evaluate the process the bank employs to ensure reliable and accurate network and data access control.

Vendor Management

1. Assess management's due diligence activities prior to vendor selection. Consider whether:

   - Strategic and business plans are consistent with outsourcing activity.
   - Senior management and the board of directors are involved in outsourcing decisions and vendor selection.
   - Vendor information was gathered and analyzed prior to contract. Determine whether management considers:
     - Vendor reputation.
     - Financial condition.
     - Costs for development, maintenance, and support.
     - Internal controls and recovery processes
     - Service level agreements.
     - Vendor and bank management responsibilities.

2. Determine whether the bank has reviews vendor contracts to ensure that the responsibilities of each party are appropriately identified.

3. Determine whether contracts address topics in the "Contracts" section of the *FFIEC Information Systems Examination Handbook*. Note whether vendor contracts provide or consider:

   - Description of the work to be performed or service provided.
   - Basis for costs and description of additional fees.
   - Online communications and availability, transmission security, and transaction authentication.

- Audit rights and responsibilities.
- Contingency plans for service recovery and data backup and protection provisions.
- Liability for data and confidential treatment of information.
- Hardware and software upgrades and price changes.
- Availability of financial information.
- Training and problem resolution.
- Reasonable penalty and cancellation provisions.
- Prohibition of contract assignment.

4. Determine whether the bank obtains and reviews internal or external audit reports evaluating vendor management processes or specific vendor relationships as they relate to information systems and technology.

5. Determine whether management designates personnel responsible for vendor management. Note management's responsibilities and whether they are held accountable for monitoring activities and services.

6. If the institution is a provider of Internet banking software products, determine whether management has an adequate process to determine who maintains the program source code.

7. If the institution obtains software products from a vendor, determine whether the bank has an adequate process to ensure that software maintained by the vendor is under a software escrow agreement and that the file is confirmed as being current on a regular basis.

8. If the vendor has dial-in capability to the bank's systems for diagnostic or maintenances purposes, determine whether the bank has an adequate process to ensure that the vendor's activities are well controlled and whether fidelity insurance extends to the vendor's employees.

Passwords

1. Assess the adequacy of the process for password administration for Internet banking systems. Consider the following:

- The adequacy of control and security over the bank's process for issuing passwords to customers.
- Whether alphanumeric passwords are required.
- The required length of passwords.
- Whether passwords have an automatic expiration.
- If adequate procedures are in place for resetting passwords.
- If automatic log-off controls exist for user inactivity.
- Whether excessive failed access attempts by the user disables access.

2. Evaluate the adequacy of the process used to select how passwords are employed to authenticate users including whether:

   - Controls combine passwords with other authentication techniques.
   - Password-only log-in is used for access control and authentication.
   - Password-only log-in is used for public network (Internet) access. If so, determine whether the institution has compensating controls to authenticate users.

Firewalls

1. Evaluate the process management uses to determine the appropriate type of Web site (informational, communicative, or transactional) for the bank's Internet-based banking business.

2. Determine whether the institution has a sound process to ensure adequate control over the path between the Web site and the institution's internal networks or computer systems.

3. Determine the process management employs to ensure that the firewall, if used, prevents unauthorized access to internal networks and computer systems.

4. If the firewall was commercially purchased, determine whether the bank has an adequate process to ensure that the responsibilities of the bank and vendor are well defined.

5. Determine the adequacy of the administration of the bank's firewall configuration and whether it ensures that:

   - Software change control procedures are appropriate.
   - Vendors provide timely fixes or upgrades and whether management implements them in a timely manner.
   - Changes in firewall configuration are tested prior to implementation.
   - Operating system control features have been invoked.
   - Operating system software default settings are adequate.

6. Determine whether the bank has an adequate process for:

   - Conducting penetration testing and certification.
   - Reviewing the qualifications of the company/person performing the certification.

7. Determine whether the bank has an effective process to assess the adequacy of physical controls in place to restrict access to firewall servers and components.

8. Determine whether the institution has an adequate process to identify any remote access, other than through a firewall, and how management monitors and controls that access.

9. Determine the adequacy of the institution's process to restrict access to firewall configuration documentation.

Physical Security

1. Determine whether the bank has an adequate process to address physical security for hardware, software, and data communications equipment associated with the Internet banking system including:

   - Whether the network servers are secured.
   - How the institution prevents unauthorized physical access to equipment.
   - Whether the bank secures vendor owned equipment.
   - If proper physical controls are in place for the data center or other location housing equipment and documentation.

Transaction Verification

1. Determine whether the bank has an adequate process to verify transactions to avoid claims of repudiation by bank customers.

Encryption and Confidentiality

1. Determine whether the bank has an adequate process to select encryption appropriate for its environment and whether the encryption selected is structured upon public, private, or a hybrid encryption system. Note the following:

   - The type of algorithm used and what it is used for.
   - Whether bank uses a proprietary or unknown algorithm.
   - The key length used for encryption, *e.g.,* 56-bit.
   - Whether encryption is used to secure passwords during transmission or storage.
   - Whether encryption is used to protect sensitive stored data.

2. If the bank engages in international banking activity, determine whether the bank is aware of U.S. government exportation policies and related restrictions controlling the exportation and use of encryption technology.

3. Determine whether the bank has an adequate process regarding the collection and use of personal information necessary to protect customer privacy (see AL 99-6).

Virus Detection and Prevention

1. Determine whether the bank has an adequate process regarding virus detection and prevention associated with the Internet banking systems. Consider whether:

   - User awareness efforts address viruses.
   - The last risk assessment and/or audit reports identified any deficiencies in virus controls.
   - The frequency with which anti-virus products and definitions are updated and whether the most current version/release is installed.

2. Determine whether the bank has an adequate process regarding virus detection and prevention. Consider whether:

   - Virus detection software distribution is made through downloads from the bank's server.
   - The bank's software distribution process provides for virus detection/prevention.

Business Resumption and Contingency Planning

1. Determine whether there is an adequate process to develop and review the bank's business impact analysis. Consider whether:

   - Internet banking is viewed as a critical business or product line.
   - Management has reviewed the impact to the bank's reputation if its Internet banking products and services are not operable.

2. Determine whether the bank has an adequate process to develop and test the contingency and business resumption plans for Internet banking products and services including whether:

   - The contingency and business resumption plans provide adequately for recovery.
   - Contingency and business resumption plans are appropriately tested on a regular basis.

3. Determine whether the bank has an adequate process in place for Internet banking recovery including whether:

   - Internet banking contingency and business resumption plans are reviewed and updated regularly.
   - Specific personnel and staff are responsible for initiating and managing Internet banking recovery plans.
   - The plan ensures that single points of failure for critical network points are adequately addressed.
   - The plan establishes strategies to recover hardware, software, communication links, and data files.

- Adequate back up agreements and contracts are in place for external vendors or critical suppliers and if these backup arrangements are tested fully.
- The response process assures that senior management and the board of directors are made aware of adverse events as dictated by the severity of damage and monetary loss.
- Outreach strategies are adequate to inform the media and customers of corrective measures.
- Legal liability issues are contemplated and addressed as part of response processes.
- Procedures are in place to bring security breaches to the attention of appropriate management and external entities (e.g., Computer Emergency Response Team (CERT), FBI, OCC, etc.).

4. Determine whether the bank has an adequate process to review the results of the most recent contingency and recovery plan testing including whether management:

   - Requires annual testing of recovery processes and systems.
   - Addresses adverse test results in a timely manner.
   - Informs the board or executive management of test results.

Personnel

Objective: Given the size and complexity of the bank, determine whether bank management and personnel display acceptable knowledge and technical skills to manage Internet banking.

1. Through discussions with management, determine their level of technical knowledge and assess the adequacy of that knowledge for the size and scope of the bank's Internet banking operations.

2. Assess technology related training programs and security awareness efforts including whether:

   - Management provides timely technical training opportunities.
   - Management measures the effectiveness of security awareness.
   - Bank staff and Internet banking users are aware of security responsibilities and bank policies.

- Management relies, solely or in part, on external vendors for technical expertise.

Controls

Objective: Determine whether management has instituted controls that are appropriate to the type and level of risks arising from Internet banking.

Digital Signatures and Certificate Authorities (CA)

1. Determine whether management requires use of digital signatures to authenticate the bank, users, and transactions.

2. Determine whether digital signatures are issued, managed, and/or certified by an external vendor.

3. If the bank is acting as its own certificate authority note:

   - Whether the digital signature system is open or closed.
   - Whether the bank has written policies and procedures for issuance, renewal, and revocation of certificates.
   - How the institution establishes and verifies credentials of subscribers.
   - Whether administrative reporting systems are adequate to provide for directory lookup and auditing (i.e., time stamping).
   - Whether the CA facility or area is adequately secured including whether:
     - Controls are in place to protect servers housing CA information and directories.
     - Contingency plans accommodate customer needs in case of system failure or disaster.
     - The bank has addressed the legal implications of providing a CA function.
     - The CA conforms to established standards (*e.g.,* NIST or IETF).
     - An audit process is in place.
   - Whether limitations have been established for certificates such as:
     - The number of transactions.
     - The type of transactions.
     - Expiration dates.
   - Whether the CA establishes classes of certificates based on message or transaction sensitivity.
   - Whether the bank is staying current on applicable laws.

- Whether the bank periodically performs a cost/benefit analysis of the business.

Biometric Devices

1. Determine whether the institution uses biometric devices for authentication purposes.

2. Determine whether a risk assessment, audit, or cost/benefit analysis has been performed of biometric devices used for authentication purposes.

3. Determine whether acceptable biometric tolerances and policies have been established for authenticating the transaction to be processed.

4. Obtain and review management reports that address statistical performance of the biometric authentication devices in service.

Monitoring

1. Discuss with management the techniques used to monitor the security of Internet banking systems. Obtain and review sample reports such as:

   - Penetration test scope and results.
   - Security violation information.
   - Real-time intrusion detection reports.
   - Reports depicting security breaches or system intrusion.

2. Determine whether security analysis software is used and note its capabilities.

3. Determine whether management conducts or has employed outside vendors to conduct penetration testing. Assess whether:

   - An objective party performs penetration testing.
   - Persons performing the tests are appropriately bonded.
   - Penetration testing is performed at least annually or at an acceptable frequency based on management's risk analysis and risk tolerance.
   - Test information and documentation is strictly controlled.

4. Determine how management monitors and detects internal or external network intrusion including whether:

   - Monitoring software is used to track real-time network traffic.
   - A qualified individual is responsible for regularly monitoring network traffic.
   - Activity logs are maintained and reviewed on a regular basis.
   - Intrusion detection techniques allow for immediate notification of network administrators or security personnel.
   - Security policies define reportable events.
   - Processes are incorporated to assure appropriate levels of management, directors, and external authorities are notified.

5. Determine through review of reports or inquiries of management whether the bank has experienced any of the following occurrences. If so, document in work papers:

   - Any alteration of the bank's home page.
   - Any unauthorized access from external or internal sources.
   - Financial damage incurred as a result of any unauthorized intrusion. If losses have been sustained, determine if the bank filed a suspicious activity report per OCC Advisory Letter 97-9, "Reporting Computer-Related Crimes."

6. Determine whether management has emergency response procedures and evaluate whether they are effective in handling an unauthorized intrusion. Discuss and document controls for remote access including whether:

   - Security policies address remote access.
   - Staff is aware of policies and adherence is monitored.
   - Audit logs are maintained to monitor remote access.

Performance Monitoring

1. Determine how management monitors system performance (e.g., transaction volume, response times, availability/downtime, capacity reports, and customer service logs and complaint summaries).

2. Determine how management projects future systems needs to ensure continued availability of the network to meet customer demands.

Customer Support

1. Evaluate the role and quality of customer service and support for Internet banking products and services.

2. Review the organization and responsibilities of the customer support function.

3. Determine whether the customer support service is outsourced. If so, note the responsibilities of the vendor and determine how management monitors customer problems, demands, or complaints.

4. Determine whether customer service levels have been established. If so, determine how management monitors adherence to service levels.

5. Determine how management assesses the adequacy of customer service.

6. Through reviews of problem logs or customer service reports and discussion with management, determine whether deficiencies exist in the process.

7. Determine whether customer service is considered in Internet banking growth projections and resource planning.

Software Distribution

1. Determine whether program change controls exist and whether they are adequate to prevent unauthorized software alterations including whether:

   - Approval procedures exist to initiate program changes and whether they are at critical points throughout the development process.
   - Procedures are followed for emergency and temporary software fixes, and new releases.
   - Change control documentation provides adequate audit trails and support for software changes.

2. Evaluate version control and software distribution procedures associated with Internet banking applications including:

   - The adequacy of software distribution (automatic download, user initiated download, or manual delivery).
   - Whether adequate controls are in place to guard against virus infection during distribution and to ensure the integrity of software.
   - Whether software testing is performed prior to distribution.

Audit

1. Determine whether the scope of internal or external audit coverage includes Internet banking.

2. Determine whether a risk assessment or audit has been performed on key management practices. Review applicable reports.

3. Determine whether internal audit is or was involved in planning and implementing the Internet banking system.

4. If available, obtain internal or external audit reports (including Type II SAS 70 reviews) that evaluate vendor management processes or specific vendor relationships as they relate to information systems and technology.

5. Obtain management reports or conduct interviews with management to determine whether vendor controls have been evaluated. Determine whether management has considered the adequacy of:

   - Security controls and reporting including whether management understands and has evaluated security for access control, user authentication, and data privacy.
   - Security monitoring activity including whether the vendor performs real-time intrusion detection and penetration testing of offsite or in-house networks.
   - Service levels and the vendor's ability to meet negotiated standards.

- Testing activity by the vendor prior to product distribution.
- Virus detection processes.
- Contingency planning and business resumption plans.

6. If the bank outsources its Internet banking processing, determine the name of the vendor(s) employed and whether the bank has obtained and reviewed the regulatory agency examination report of the vendor.

7. Determine whether the audit function reviews the consistency between the bank's disclosed security and privacy standards and actual bank practices.

Internet Service Providers (ISP)

1. Determine whether the bank relies on a third party Internet service provider (ISP) to support access to Internet banking services. If so, note whether management's supervision of the vendor includes:

   - Determining whether performance meets service level agreements.
   - Requiring the ISP to monitor bank Internet links and report to them when these links are down or unavailable.
   - Determining the ISP's contingency planning and business recovery capabilities.
   - Identifying whether the ISP has adequate support staff.
   - Determining whether the bank is subject to differing service access types that may cause less than acceptable support.
   - Determining whether the ISP provides bank-defined filtering or establishes its own firewall-filtering parameters.
   - Determining whether the ISP has sound controls over changes to the bank's Internet address.
   - Assessing the soundness of the ISP's financial condition.
   - Reviewing the ISP's security standards and practices.

2. Determine whether the bank has alternate data communications paths in the event the primary ISP is unable to handle the bank's Internet traffic due to a malfunction or inadequate capacity.

Conclusion Procedures

Objective: Communicate findings and initiate corrective action on violations and other deficiencies.

1. Prepare a summary memorandum detailing the results of the Internet banking examination. Draft conclusions on:

   - The quantity of risk.
   - The quality of risk management.
   - The direction of risk.
   - The extent to which risk management practices affect aggregate risk.

2. Also address in the summary memorandum:

   - Appropriateness of strategic and business plans.
   - Adequacy and adherence to policies.
   - Adequacy of MIS.
   - Compliance with applicable laws, rules, and regulations.
   - Adequacy of internal controls.
   - Recommended corrective action regarding deficient policies, procedures, practices, or other concerns.
   - The institution's Internet banking prospects.
   - Other matters of significance.

3. Discuss examination findings and conclusions with the EIC. If necessary, compose "Matters Requiring Board Attention" (MRBA). MRBAs should cover practices that:

   - Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
   - Result in substantive noncompliance with laws or regulations.

   MRBA should discuss:

   - Causes of the problem.
   - Consequences of inaction.

- Management's commitment to corrective action.
- The time frame and person(s) responsible for corrective action.

4. Discuss findings with management including conclusions regarding applicable risks. If necessary, obtain commitments for corrective action.

5. As appropriate, prepare a Internet banking comment for inclusion in the report of examination.

6. Write a memorandum specifically stating what the OCC should do in the future to effectively supervise Internet banking in this bank. Include supervisory objectives, time frames, staffing, and workdays required.

7. Update the electronic information system and any applicable report of examination schedules or tables.

8. Update the examination work papers in accordance with OCC guidance.

Firewalls and Associated Controls

The purpose of this appendix is to provide background material on the fundamentals of firewalls and their use in banking and electronic commerce.

Examiners and other readers of this section should familiarize themselves with the *FFIEC Information Systems Examination Handbook* (*IS Handbook*) chapters on Security and Networking. This discussion assumes a knowledge of the content of the *IS Handbook*, specifically the section dealing with networks.

Management needs to understand the capabilities and functionality of the firewall and make sure that their systems are configured appropriately for the bank's business needs. Ongoing monitoring of the firewall ensures that the appropriate functions and utilities are activated to protect the institution and prevent attacks against known system weaknesses. Institutions that do not have the expertise to design, install, and test firewalls should seriously consider engaging professionals to perform this function. Due care should be exercised when selecting the vendors to perform these functions and sound internal controls should be in place along with audits to verify the vendor's activities with the firewall. The institution should periodically engage an independent source to test the firewall for weaknesses. This includes annual, or more frequently as circumstances warrant, penetration testing to ensure controls are appropriate to the type and level of risk arising from the institution's Internet banking products and services.

A firewall is hardware and software placed between two networks. The intent is for all network traffic, regardless of the direction of flow, to pass through this firewall. The firewall then can check all traffic to make sure it is authorized and prevent unwanted traffic from entering the system. The firewall also can check the traffic to determine whether it contains any unauthorized attachments, such as viruses. Firewalls need to be efficient to catch any traffic that is unauthorized in order to prevent potential harm to the institution.

Network isolation is a function of firewalls. A domain name server converts publicly known addresses into internal addresses that are not publicly known. This is sometimes referred to as a "bastion host." The feature prevents intruders from gaining access to internal names and addresses on the bank's

internal network. External devices attempting to access internal addresses are suspect and should be screened out.

Address screening is another of the functions of a firewall. This function is used to filter-out messages with inappropriate source addresses. For example, this function would screen out messages with internal system addresses. Messages that have not gone through a domain name server should not have internal addresses and would be suspect. Such traffic should not be allowed to pass through the firewall.

Application screening is a firewall function used to prevent inappropriate instructions from entering the system or an unauthorized access to the administrator level of the server. A "proxy server" is a device used to test the system's "rules" to prevent deviations from the established rules.

Message flow inspection or state full inspection is a function of a firewall used to detect inappropriate responses by the system. The system creates a database and looks for inappropriate responses by a server to messages or inquiries. For example, if a request asks for account balance information and the response is to transfer funds, the "state full inspection" will recognize an inappropriate response and terminate the session.

Other controls normally work in tandem with firewalls. These controls include logical access controls and physical security. The reason these controls are important is that insiders represent the greatest threat to bank computer systems and data communications networks. Various studies reflect that nearly 70 percent of intrusions originate within the organization. Insiders have knowledge of the system or network and may have the opportunity to originate an unauthorized transaction either by accident or intent. Access to systems, networks, and information should be on a "need-to-know" basis. Banks also need to provide protection from employee ignorance such as sharing passwords and running outside software without virus checking.

A logical access control includes a user identification and a password. An individual's user ID might be J. Examiner. But each user should also have a unique password composed of at least 6-8 alphanumeric characters; more is better. It is important to avoid using passwords that are easily discerned. Names, addresses, or words found in the dictionary, any language, spelled forward or in reverse should be avoided. One option is to use mnemonics —

something that is easy to remember but difficult to guess. An example of a mnemonic is the following phrase; "Examiners are curious, bright people." The mnemonic is EACBP. By adding some numbers and/or special characters, a password can be created that is easy to remember but difficult to discern. *See* OCC Bulletin 98-38 "Technology Risk Management: Internet Banking" and the *IS Handbook* for a more complete discussion of logical access security and controls.

Physical security also is an important control function in protecting a bank's data communications networks and internal accounting systems. Network hardware should be stored in secure locations so that it is accessible only to authorized personnel. This is a preventive control to protect the bank's assets and protect the institution from transaction, reputation, and strategic risk.

Personal computers connected to a network should have sound logical access controls. This includes a password feature to access the network and time-out password controls to protect the network when a particular PC is unattended, even for brief periods of time.

Banks should consider the feasibility of centrally controlled modem pools. Controlling the placement and access to modems attached to a bank's network will help the bank limit access to only authorized individuals. Banks should specifically guard against unauthorized modems that employees may attach to their PCs which are connected to the bank's data communication network. These unauthorized modems can be targets of "random dialing" efforts and can be a vulnerable entry point into the bank's network.

Time of day controls can be used to restrict access to a bank's network to certain, preauthorized times. The objective is to limit the opportunity for after-hours access except as authorized by the network administrator. Decisions on this type of control will be based on the types of business the bank is engaged in and the need for access to its internal networks.

Well-defined policies will help a bank develop a sound system of controls and ultimately reduce the vulnerability to penetration. Well-defined control objectives will help the systems administrator or vendors to properly configure the firewall. Such policies also will give auditors a standard to measure against when performing tests. Some considerations for bank firewall policies include:

- Communicating the bank's policy with respect to monitoring employee use of data communications networks, including electronic mail and the Internet.

- Requiring virus checking for all diskettes or downloads from other than authorized sources. Even diskettes received from other employees can be contaminated with a virus and should be scanned before use, especially on a PC connected to the bank's network.

- Determining the bank's policy for the access to PCs and the bank's network after hours for uses that are not related to work.

- Informing employees of the consequences of violating the institution's network usage policies.

- Limiting access to and use of administrator level capabilities of the firewall hardware and software.

- Requiring periodic review of the vulnerabilities of the bank's firewalls from known threats including, penetration testing.

- Regularly logging and reviewing all activity.

Sophisticated auditing techniques are appropriate to determine whether effective policies are in place and whether the system of controls over the bank's networks are working as intended. The controls and audits of firewalls need to be performed on a regular basis. Firewall systems are dynamic and need regular reviews to ensure protection from newly identified vulnerabilities and system weaknesses.

Once the internal or external auditor gains a sound understanding of the bank's network configuration and types of business, he or she may decide to perform various tests to ensure the soundness of logical access controls. This might include testing default settings to determine whether only authorized firewall functions are permitted. The auditors might use audit software to scan the activity logs looking for anomalies or unusual activity. They might review the screening of employees who developed or installed the network. The auditors

might also review the frequency of password changes for employees authorized access to a bank's data communications network.

Depending on the level of Internet banking employed, the bank will want to consider engaging outside experts to review their security measures and offer recommendations for enhancements. This type of review should be considered at least annually for transaction systems and somewhat less frequently for communicative and informational systems.

Examiners will find a more complete discussion of these issues in the *IS Handbook*.

Cryptography

This appendix provides background material on the fundamentals of cryptography and the uses of encryption in banking and electronic commerce.

Business, including banking, is shifting from paper based or physical processes to electronic based or digital processes. This includes retail delivery of products and services, electronic data interchange, wholesale funds transfer, clearing, settlement, and Internet banking. Bank managers will need to engineer sound controls into these new business models to manage risk. While all of this is taking place, the basic needs for data privacy, trust, and verification will continue in the digital world as it has in the physical world. Encryption offers possible solutions.

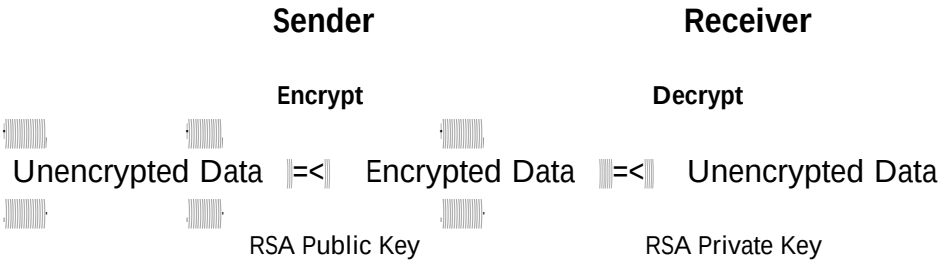
Different Kinds of Encryption

Two different kinds of encryption exist with two separate purposes. One purpose is to keep information private. The other is to verify the identity of parties in a transaction. Both kinds of encryption are typically used together to both protect messages and validate the parties involved. Each is governed by industry standards. Vendors provide the encryption technology as software products or as part of specific hardware devices. These two fundamental types of encryption are symmetric and asymmetric.

Symmetric, also known as secret key cryptography, requires both the sender and receiver to have the same key (the integers that drive the encryption algorithm). The diagram on the following page shows how the process works. The sender encrypts the message and the receiver decrypts the message using the same key. One of the most commonly used systems of this type is the Data Encryption Standard, or DES. The U.S. Government adopted this IBM- developed technology in 1977. It is widely used and operates on a minimum 56 bit (binary digit) base key. Some institutions will use Triple-DES where the message is encrypted three times to enhance its resistance to decoding.

The advantages of secret key cryptography are that it is secure, widely used, and fast. The disadvantages are that key administration is complex, requiring both parties to maintain absolute control over exchanging keys, it does not include a separate authentication mechanism, and there is no non repudiation (undeniable proof of participation of the sender and receiver). In addition, some cryptographic systems are subject to export restrictions from the U.S. government.

Asymmetric, also known as public/private key cryptography, employs two keys. As noted in the following diagram, in order to secure a message the sender performs the encryption using the recipient's public key. However, the receiver can only read the information using their private key. Often the literature refers to this technology as two key cryptography. A popular public key technology is RSA. Ron Rivest, Adi Shamir, and Leonard Adleman developed RSA in 1977. The primary use of RSA is for authentication and the secure exchange of encryption keys and digital signatures. Key length can vary from 40 to 1,024 bits.

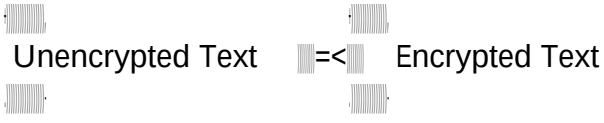


Some of the advantages of public key cryptography over private key cryptography are that it simplifies key administration. For example, there is no requirement for a prior relationship between the sending and receiving parties. In addition, the key lengths can be much longer than DES. According to the vendors, this makes public key cryptography stronger. It also provides for non repudiation. The major disadvantage is that public key is much slower than private key cryptography. Thus, it is used primarily to authenticate messages rather than encrypt an entire message.

How Encryption Works in Practice

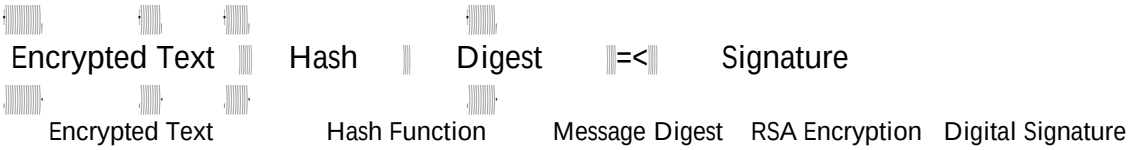
Encryption may be used to both secure the message and authenticate the sender. The normal approach is to use the asymmetric and symmetric encryption technologies in tandem. Symmetric encryption is typically used for encrypting large volumes of information and asymmetric encryption is for authentication. This is because the symmetric technology is up to 10,000 times faster than the asymmetric technology. The following is an example of how this works:

> If FNB wants to send a secure message to its correspondent, FNB needs to do two things. First, FNB needs to make sure the message is secure. FNB might do this by using DES or Triple DES (symmetric or secret key) to encrypt the message.



DES Encryption

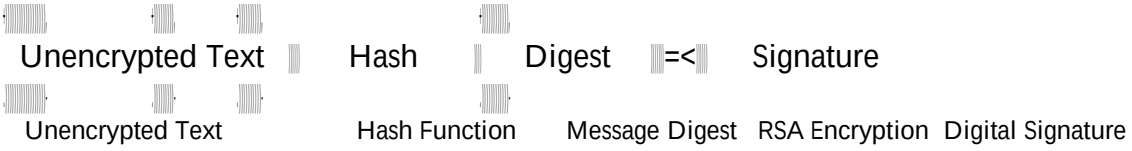
Second, FNB will authenticate themselves thus providing an assurance to the correspondent that the message came from FNB. FNB does this by using a hash function (a mathematical function derived from the message) to create a message digest from the text. Using RSA (asymmetric or public/private key), FNB then encrypts the message digest using its RSA private key. The correspondent can only read the encrypted message digest using FNB's public key. Thus, the recipient knows the message came from FNB.



When the correspondent receives the message, the correspondent then uses FNB's public RSA key to decrypt the message digest. The correspondent compares the decrypted hash total to one they have independently calculated from the message. If the hash totals agree, the correspondent has a high level of assurance that the message came from FNB and that nothing was lost or tampered with during transmission. The correspondent can then use the DES key to decrypt the text of the message.

Not every message needs the security or privacy provided through encryption. In addition, some countries will not allow encrypted messages to travel across their borders. Message authentication can be used in these situations. Message authentication is a technique used to attach a digital signature to a transmission.

In the example below, if the correspondent wants to send a message to FNB but the correspondent is located in a country that does not permit message encryption, the correspondent can use message authentication to assure FNB that the message came from them. From the text of the message, the correspondent will first use a hash function to create a message digest. Next, the correspondent will use their private key to encrypt the message digest to create a digital signature. The encrypted message digest can only be read using the correspondent's public key. Accordingly, FNB will use the correspondent's public key to decrypt the message digest and compare the hash total to one they have independently calculated. If they agree, FNB has a high level of assurance that the message came from the correspondent and that, even though the message was sent in clear text, nothing was lost or tampered with during transmission.



This is the same process for adding the digital signature for the encrypted DES message above. However, when used with an unencrypted or clear text

message, the process is called message authentication. This process is sometimes referred to as a digital envelope, a digital message protected by a digital signature.

Types of Online Attacks

Banks and service providers need to guard against various types of online attacks. The object of an attack may vary. Attackers may try to exploit know vulnerabilities in particular operating systems. They also may try repeatedly to make an unauthorized entry into a Web site during a short time frame thus denying service to other customers.

Types of attacks may include:

- Sniffers — Also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture log-on IDs and passwords.

- Guessing Passwords — Using software to test all possible combinations to gain entry into a network.

- Brute Force — A technique to capture encrypted messages then using software to break the code and gain access to messages, user ID's, and passwords.

- Random Dialing — This technique is used to dial every number on a known bank telephone exchange. The objective is to find a modem connected to the network. This could then be used as a point of attack.

- Social Engineering — An attacker calls the bank's help desk impersonating an authorized user to gain information about the system including changing passwords.

- Trojan Horse — A programmer can embed code into a system that will allow the programmer or another person unauthorized entrance into the system or network.

- Hijacking — Intercepting transmissions then attempting to deduce

information from them. Internet traffic is particularly vulnerable to this threat.

Discussion Points

There are several topics examiners can discuss with bankers who are considering engaging in Internet banking for the first time. These talking points will help the examiner determine if fundamental risk issues are under consideration.

- Strategic Plans — The proposed Internet banking business should be a good fit with the institution's strategic business direction and customer demographics.

- Hosting — One of the major decisions a national bank will have to make is whether to host the service in-house or through an outsourcing arrangement.

- Functionality — A needs analysis can help the bank determine what products and services should be a part of the new Internet banking business. This should be an on-going process to ensure the bank remains current with Internet banking technology, products, and services.

- User Department — The bank's user departments should be involved in the outsourcing vendor or software vendor selection process as these individuals will have to work with the system on a daily basis once it is operational.

- Impact on Earnings and Capital — Bank management should have a projection of the expected impact on earnings and capital of the new Internet banking business.

- Security — Bank management needs to understand security issues associated with Internet banking products and services. Security issues

include how the bank or its outsourcer will authorize users, prevent data interception and unauthorized alteration, and deal with intrusions.

- Internal Controls and Audit — Management should determine whether the controls and audit processes are adequate to enable the identification, measurement, and monitoring of risk associated with the Internet banking business.

- Legal Requirements — Various legal requirements, including compliance issues, need to be understood before initiating an Internet banking business. Since many legal issues are undecided, management will need to monitor developments.

- Vendor Management — If the bank is researching outsourcers, the analysis should include consideration of potential vendors' financial condition, years in the business, and future plans.

- Contingency planning — Whether provided by the bank or outsourcer, management should have an understanding of contingency planning as part of the due diligence process.

- Insurance — A review of insurance coverage may be in order especially if the hosting of the Web site has been outsourced.

- Consultants — The bank should ensure they have the proper level of expertise to make this business decision. The board and senior management may need to enhance their understanding of technology issues. If the expertise is not available in-house, the bank should consider engaging outside expertise.

Since these are dynamic discussion points, examiners should periodically reference the Bank Technology Division Intranet site for updates.

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.
Access Control List (ACL)	List of security identifiers that allow only certain processes to be activated.
Access Products	Products that allow consumers to access traditional payment instruments electronically, generally from remote locations.
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.
Automated Clearing House (ACH)	An automated clearing and settlement system for recurring payments. Most ACH systems are operated by the Federal Reserve Banks.
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.
Alerter Service	Notifies selected users and computers of administrative alerts that occur on a computer.

Algorithms	Mathematical formulas used to encrypt and decrypt messages. These encryption formulas can reside in software or specialized hardware devices.
Alpha Test	The first stage of testing a new software product, carried out by the manufacturer's technical staff.
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.
American National Standards Institute (ANSI)	A standard-setting organization; it is the U.S. representative to the International Standards Organization (ISO).
American Standard Code	A standard code for representing characters as numbers that for Information Interchange is used on most microcomputers, computer terminals, and printers.
Applet	A small application program that is designed to do a small, specific job.
Application	A computer program or set of programs that perform the processing of records for a specific function.
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.

Asynchronous Transfer Mode	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.
Auditability	The degree to which transactions can be traced and audited through a system.
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.
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.
Authoring Software	Software used to produce multimedia or hypertext presentations by linking sounds, music, visuals, and text.
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, he or she may be authorized different types of access or activity.
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.
Bandwidth	The transmission capacity of a computer channel or communications line.
Bastion Host	A firewall system that has been designed 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.
Baud Rate	Measurement of data transfer speed.
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.
Biometrics	A method of verifying an person's identity by analyzing a unique physical attribute.
BIT	A binary digit (0 or 1) used in the representation of a number, letter, or special character.
Bridge	In local area networks, a device that enables two networks, even ones dissimilar in topology, wiring, or communications protocols, to exchange data.
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.

Bundled Software	Software that is sold in combination with hardware.
CERT	See Computer Emergency Response Team
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.
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.
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.
Cipher Text	An encrypted message that outsiders cannot read.
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.

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.
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.
Client-server Network	A network that dedicates certain computers called servers to act as service providers to computers called clients.
Closed Network	A data communications 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).
Code	Computer programs, written in machine language (object code) or programming language (source code).
Computer Emergency Response Team (CERT)	Located at Carnegie-Mellon University, this incident response team offers advisories that contain useful, specific security information.
Cyber Mall	A set of electronic or digital storefronts linked through a common Web site.
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.
Cryptography	The art/science of keeping messages secret from outsiders.

Data Encryption Standard	DES is a well-known symmetric encryption standard that the U.S. Government endorsed in 1977. Developed by IBM, it operates off of a 56-bit base key.
Data Integrity	The property that data meet with a priority expectation of quality and that the data can be relied upon.
Dedicated	Assigned to only one function.
Default Shares	Resources shared by default when the operating system is installed.
Denial- of- Service Attack	An attempt to overwhelm a server with requests so that it cannot respond to legitimate traffic.
Design Phase	The phase of systems development 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.
Design Specification	A baseline specification that defines how to construct a computer-based business system.
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.
Dial-up	The ability of a remote user to access a system by using private or common carrier telephone lines.

Dial-up Client	A computer with a temporary connection to the Internet.
Digital	Referring to communications processors, techniques, and equipment where information is encoded as a binary “1”or “0”.
Digital Certification	A process to authenticate (or certify) a party’s digital signature; carried out by trusted third parties.
Digital Envelope	A digital message protected by a digital signature.
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.
Domain	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
Domain Controller	The server that authenticates domain logins and maintains the security policy.
Domain Name	An alphanumeric name for a Web site that includes both the online address and online name.
Domain Name Service	A network service that translates

(DNS)	external Internet addresses into numerical Internet network addresses.
Download	To transmit a file or program from a central computer to a smaller computer or to a remote site.
Dynamic Host Configuration	Method of automatically assigning addresses to client computers on a network.
Electronic Benefits Transfer (EBT)	The electronic delivery of government benefits using plastic cards.
Electronic Data Interchange (EDI)	The transfer of information between organizations in machine readable form.
Electronic Document	The digital or computer equivalent of paper documents.
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.
Electronic Purse	A stored value device that can be used to make purchases from more than one vendor.
Feasibility Analysis	The process of determining the likelihood that a proposal will fulfill specified objectives.
File Transfer Protocol (FTP)	A standard way of transferring files from one computer to another on the Internet.
Firewall	A system or combination of hardware and software solutions that enforces a boundary between two or more networks.

Gamma Test	The third stage of software testing completed before release.
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.
Gopher	A computer program, and an accompanying data transfer protocol, for reading information that has been made available to users on the Internet.
Graphical User Interface (GUI)	A way of communicating with a computer by manipulating icons and windows with a "mouse."
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.
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.
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.

Hardware Compatibility	A listing of all hardware devices supported by the operating system.
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.
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.
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.
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.
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.
Hypertext	Electronic documents that present information that can be connected together in many different ways, instead of sequentially.

Hypertext Markup Language (HTML)	A set of codes that can be inserted into text files to indicate special typefaces, inserted images, formatting, and links to create Web pages.
Hypertext Transfer Protocol	HTTP is a standard method of publishing information as hypertext in HTML format on the Internet.
Icon	A small picture on a computer screen that represents a particular object, operation, or group of files.
IDEA	International Data Encryption Algorithm.
IETF	Internet Engineering Task Force: a standards-setting organization.
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 compromises.
Integrated Circuit Card	A plastic card in which one or more integrated circuits are embedded (also called a chip card).
ISDN	Integrated Services Digital Network. A type of all-digital telephone service that can transmit digital data as well as voice, without a modem.
ISO/OSI	An international standard-setting organization. ANSI is the U.S. representative.
Internet	A worldwide network of computer networks (commonly referred to as the Information Superhighway).

Internet Information Server	Software used to serve higher-level Internet protocols, like HTTP and FTP for clients using Web browsers.
Internet Service Provider (ISP)	An entity that provides access and/or services related to the Internet, generally for a fee.
Interoperability	The compatibility of distinct applications, networks, or systems.
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.
Kernel	The core process of a preemptive operating system, generally consisting of a multitasking scheduler and the basic security services.
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.
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.
Lock and Key Protection	A protection system that involves matching a key or password with a specific access requirement.
Logging	The storing of information about events that occurred on the firewall or network.
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.
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.
Magnetic Stripe	Used on debit, credit, and identification cards to store encoded information read by card readers; less secure than computer chip cards.
Memory Card	An integrated circuit (IC) card capable of storing information only.
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.
Middleware	Facilitates the client/server connections over a network and allows client applications to access and update remote databases and mainframe files.
Multimedia	The combining of different elements of media (i.e., text, graphics, audio, video) for display and control from a personal computer.
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.
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.
National Institute for Standards Technology	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).
National Security Agency (NSA)	Responsible for government and/or military information security.
National Telecommunications Information Administration	A government agency charged with safeguarding personal information on U.S. citizens.
Navigation	Moving through a complex system of menus or help files.
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.

New Technology (NT)	A Microsoft operating system.
Node	Any device, including servers and workstations, connected to a network. Also, the point where devices are connected.
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.
Nonrepudiable Transactions	Transactions that cannot be denied after the fact.
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.
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.
Off-line	Equipment or devices that are not in direct communication with the central processor of a computer system, or connected only intermittently.
Online	Equipment or devices that are currently capable of communicating with one relevant computer system.
Online Scrip	Debit accounts on the Internet or other major computer network.
Online Service Providers	Closed network services that provide access

(OSP)	to various computer sites or networks for a fee.
Open Network	A data communications network to which access is not restricted.
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.
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.
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.
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.
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.

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.
Password Sniffer	A software program that is illicitly inserted somewhere on a network to capture user passwords as they pass through the system.
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.
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.
Penetration Testing	Using automated tools to determine a network's vulnerability to unauthorized access.
Permission	A rule associated with an object to regulate which users can access the object and in what manner.
Personal Identification Number (PIN)	A sequence of digits used to verify identify.
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.
PGP	Pretty Good Privacy data encryption algorithm.

Piggyback	A means of gaining unauthorized access to a system through another user's legitimate connection.
Plain Text	An unencrypted message.
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).
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.
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.
Privacy-Enhanced Mail	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.
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.
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.
Proximity Cards	Cards that can be read from a short distance; mainly used for security and vehicle identification.
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.
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.
Real Time Monitoring	The monitoring of activity as it occurs rather than storing the data for later review.
Registry	A database repository for information about a computers configuration, including the hardware, installed software, environment settings, and other information.
Remote Access	Letting off-site users access a central network.
Remote Payment	A payment carried out through the sending of payment orders or payment instruments.
Remote Procedure Calls	A network interprocess communication mechanism that allows an application to be distributed among many computers on the same network.
Repudiation	The denial by one of the parties to a transaction of participation in all or part of

	that transaction or of the content of the communication.
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.
Router	A computer system in a network that stores and forwards data packets between local area networks and wide area networks.
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.
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.
Scattering	The process of mixing the integrated circuit (IC) chip components so that they cannot be analyzed easily.
Search Engines	Software programs that are capable of locating specified information or Web sites on the Internet.

Searchware	Software used to search through a database.
Secure Hypertext	Provides secure communication mechanisms between an HTTP Transfer Protocol client-server pair.
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.
Secure Socket Layer (SSL)	A protocol for providing data security during transmission using data encryption, server authentication, and message integrity.
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.
Security Policies	The security policy consists of the Account, User Rights, Audit, and Trust Relationships policies, and are managed with User Managers for Domains.
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).
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.
Settlement	An act that discharges obligations with respect to funds or securities transfers between two or more parties.
Settlement system	A system used to facilitate the settlement of transfers of funds.
Simple Mail Transfer	A protocol used to transfer electronic mail between computers on the Internet.
Smart Card	A card with a computer chip embedded, on which financial, health, educational, and security information can be stored and processed.
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.
Specification	Documents that contain basic detailed data.
Spoofing	An attempt to gain access to a system by posing as an authorized user.
Standards	The rules under which analysts, programmers, operators, and other personnel in an information service organization work.
Stored Value Card	A card that stores prepaid value by magnetic stripe or computer chip.
Structured Query Language	A query language used to manipulate large

(SQL)	databases.
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.
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.
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.
Switch	A type of bridge that can move several packets at the same time.
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.
Systems Analysis	The performance, management, and documentation of the four phases of the life cycle of a business system: study, design, development, and operation.
System Flowchart	A flowchart diagraming the flow of work, documents, and operations in a data processing application.
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.
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.
System Specification	A baseline specification containing all the essential computer-based business system documentation. It is completed at the end of the Development Phase.
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.
Tamper-evident	The capacity of devices to show evidence of physical attack.
Tamper-proof	The proven capacity of devices to resist attacks.
Tamper resistant	The capacity of devices to resist physical attack up to a certain point.
Telecommunications	Data transmission between a computing system and remotely located devices by telephone lines, cable, or wireless technology.
Telnet	A protocol that permits users to access a remote terminal or another computer through a network; widely used on the Internet.

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.
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.
Throughput	The total amount of useful work performed by a data processing system during a given period of time.
Topology	The arrangement of nodes usually forming a star, ring, tree, or bus pattern.
Traceability	The degree to which transactions can be traced to the originator or recipient (also referred to as auditability).
Transport Control Protocol	Also 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.
Trap Door	A concealed and unauthorized entrance into a computer operating system, designed by the programmer.
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.

Truncation	Dropping off part of a character string either to conserve space or because of limited space.
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.
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.
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.
Uninterruptible Power Supply (UPS)	Provides power to a system in case of a power outage.
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.

Uniform Resource Locator or Universal Resource Locator (URL)	A way of specifying the location of available information on the Internet.
Upload	To transmit a file to a central computer from a smaller computer or a remote location.
Usenet	A set of many news groups distributed by the Internet.
User Manager for Domains	A tool used to manage security for a domain or an individual computer. Administers user accounts, groups, and security policies.
Virtual Corporations	Corporations that have no official physical site presence, and are made up of diverse geographically dispersed or mobile employees.
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.
Vulnerability	A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security.
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.
Web Page	Information presented through a Web browser in a single view.

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.
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.
Win 16	The set of application services provided by the 16-bit versions of Windows 3.1 and Windows for Workgroups 3.11
Win 32	The set of applications services provided by the 32-bit versions of Windows 95 and NT.
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.
Windows NT Server	The Windows NT Server provides centralized management and security, advanced fault tolerance, and additional connectivity.
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.
Workgroup	A collection of computers that are grouped for viewing purposes. Each workgroup is identified by a unique name.
Workstation	A powerful personal computer.

World Wide Web (Web, WWW)	A subnetwork of the Internet through which information is exchanged by text, graphics, audio, and video.
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.

Laws, Regulations, and Rulings

Bank Service Corporation Act	12 USC 1861-1867
Computer-Related Fraud	18 USC 1030
FDIC Advertisement of Membership	12 CFR 328
OCC Interpretive Letter No. 742	
OCC Conditional Approval No. 253	
OCC Conditional Approval No. 312	
OCC Conditional Approval No. 313	

Issuances

AL 97-9, "Reporting Computer-Related Crimes"

AL 99-6, "Guidance to National Banks on Web Site Privacy Statements"

OCC 94-13, "Nondeposit Investment Sales Examination Procedures"

OCC 97-9, "Reporting Computer-Related Crimes"

OCC 98-2, "Interagency Statement on Branch Names"

OCC 98-3, "Technology Risk Management"

OCC 98-31, "Guidance on Electronic Financial Services and Consumer Compliance"

OCC 98-38, "Technology Risk Management: Internet Banking"

OCC 99-9, "Infrastructure Threats from Cyber-Terrorists"

OCC 99-20, "Certificate Authority Systems"

Other

FFIEC Information Systems Examination Handbook