

Electronic Banking Examination Procedures

FIL-14-97
February 26, 1997

TO:
CHIEF EXECUTIVE OFFICER
SUBJECT:
Examination Guidance on the Safety and Soundness Aspects of Electronic Banking Activities

With the increasing emergence of electronic banking, and the associated risks to the safety and soundness of insured financial institutions offering such products and services, the FDIC has developed electronic banking examination procedures for its staff. The examination procedures, which address the safety and soundness aspects of electronic banking, were issued to FDIC examiners on January 29, 1997, and are available to insured financial institutions on request.

This guidance represents the first of the FDIC's comprehensive four-part approach to evaluating the wide-ranging risks inherent in emerging electronic banking activities. The three remaining parts of this effort include:

- A training program has been created to educate FDIC examiners on how to use the new procedures.
- Procedures addressing the technical aspects of electronic banking are being developed for information systems specialists.
- A program to develop internal technical expertise is underway.

Financial institutions are using emerging technologies to offer existing products and services through new delivery channels and, in some instances, to develop entirely new products and services. Examples include Internet banking, electronic cash, and stored-value card systems. Some of the risks involved with these emerging technologies are unique to the new delivery channel, while others represent general risks that are similar to those in traditional banking activities.

These new technologies are dynamic and raise a wide range of supervisory issues. The FDIC does not wish to impose regulatory restrictions that may hinder the development of innovative products and services. However, the FDIC does wish to promote the continued safety and soundness of insured financial institutions, which are increasingly engaging in electronic banking activities. During a September 1996 public hearing held by the FDIC on stored-value cards and electronic payment systems, many participants sought regulatory guidance on safety and soundness issues. In response, the FDIC is making its examination guidance available to insured financial institutions.

The electronic banking examination procedures were designed to be sufficiently broad that they may be applied to a wide range of electronic banking activities. As such, certain review points may not apply to financial institutions that use or plan to use less sophisticated systems. The FDIC recognizes that risk-management programs should be designed in relation to the nature and complexity of an institution's activities.

The examination procedures focus on important safety and soundness functions such as planning, administration, internal controls, and policies and procedures, and are confined to non-technical strategic and administrative areas because they are designed for safety and soundness

examiners. Technical aspects of electronic banking systems will be referred to information systems specialists. Information systems examiners will continue to be guided by the FFIEC Information Systems Examination Handbook, which will soon be supplemented by technical procedures addressing electronic banking.

To request copies of the electronic banking examination procedures, please contact the FDIC's Public Information Center (PIC) by:

- calling (202) 416-6940 or (800) 276-6003,
- faxing (202) 416-2076, or
- writing to the PIC at 801 17th Street N.W., Room 100, Washington, D.C. 20434.

Electronic copies of the procedures in WordPerfect version 6.1 may be downloaded from the FDIC's site on the World Wide Web ([http://www.fdic.gov](#)).

For further information, please contact your Division of Supervision Regional Office or Cynthia A. Bonnette in the Washington Office at (202) 898-6583.

Nicholas J. Ketcha Jr.

Director
Attachment

Distribution: FDIC-Supervised Banks (Commercial and Savings)

Note: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, N.W., Room 100, Washington, D.C. 20434 (202-416-6940 or 800-276-6003).

ELECTRONIC BANKING

SAFETY AND SOUNDNESS EXAMINATION PROCEDURES



**Federal Deposit Insurance Corporation
Division of Supervision**

TABLE OF CONTENTS

Supplement to DOS Examination Manual

I.	Introduction	1
	The Networked Environment	1
II.	Electronic Capabilities	3
	Information-only Systems - Level I	3
	Electronic Information Transfer Systems - Level II	4
	Fully Transactional Information Systems - Level III	4
	Electronic Payment Systems	4
	Bank Roles in Electronic Payment Systems	6
III.	Risks	7
	Specific Risks to Electronic Systems	7
IV.	Risk Management	9
	Strategic Planning and Feasibility Analysis	10
	Incident Response and Preparedness	11
	Internal Routines and Controls	12
	Other Considerations	13
V.	Examination Program	13
	General	13
	Pre-examination Planning	13
	Examination Levels	13
	Examination Review Areas	14
	Report Treatment	17
	Impact on Bank Ratings	17
	Referrals to Specialists	17
	Electronic Banking Online Data Entry System	18
	Examination Workpapers	18

Electronic Banking Examination Procedures

Standards and Associated Risks	1
Core Analysis	3
Expanded Analysis	11
Impact Analysis	13

Pre-examination Letter and Request List

Electronic Banking Glossary

I. INTRODUCTION

Electronic commerce is a broad term applied to activities involving the exchange of goods or services for value over a computer network or automated system. As significant participants in the marketplace, financial institutions are becoming more aggressive in adopting electronic banking capabilities that include sophisticated marketing systems, remote banking capabilities, and stored value programs. This area is highly dynamic as emerging technologies yield a variety of delivery alternatives and innovative products and services. Electronic systems are becoming increasingly important due to:

- the increasing competition from non-bank financial services companies, the telecommunications industry, and systems or software developers;
- the demand for more efficient and convenient capabilities; and
- the widening cost and delivery differentials between electronic capabilities and traditional delivery channels.

The opportunities presented can pose significant risks to an insured financial institution. However, these risks can be mitigated by adopting a comprehensive risk management program that begins with a sound strategic plan. Risk identification and analysis should lead the board to adopt appropriate oversight and review guidelines, operating policies and procedures, audit requirements, and contingency plans.

The extent of a financial institution's risk management program should be commensurate with the complexity and sophistication of the activities in which it engages. For example, banks which offer a simple information-only site on the World Wide Web generally would not be expected to have undertaken the same level of planning and risk management as institutions that engage in more complex activities.

Note to users: This presentation introduces the concepts of electronic banking and the related safety and soundness issues. Users are encouraged to review the most recent FFIEC Information Systems Examination Handbook for discussion of related technical issues.

The Networked Environment

A computer network is simply an arrangement in which multiple computers are connected so that information, applications, and equipment can be shared. By design, networks can increase efficiency, convenience, and access; however, the design also limits the degree to which the environment can be controlled.

Network access can be through a combination of devices such as personal computers (PCs), telephones, interactive television equipment, and card devices with embedded computer chips.

The connections are completed principally through telephone lines, cable systems, and in some instances, wireless technology.

Electronic banking relies on a networked environment. It is important to note that not all networks carry the same degree of risk and that not all networks are equally vulnerable; not all networks are equally critical; and not all networks contain data that is equally sensitive. Every institution must evaluate the risk it faces and its readiness to react to those risks.

Whether the system is informational or transactional, these systems facilitate interaction between the institution and the user (generally, a customer), often with the support of third-party service providers. Phone banking, PC banking services, and stored value programs are important examples of electronic banking networks. Increasingly, financial institutions are also focusing on the opportunities presented by the Internet and World Wide Web.

The Internet is a public network of networks that can be accessed by any computer equipped with a modem. While not centrally managed, the Internet is given order through the World Wide Web which facilitates visual interfaces and links (i.e., electronic connections), to other information. The web also provides multimedia capabilities such as text, graphics, audio, and video. Intranets are private networks that are built on the infrastructure and standards of the Internet and web. Intranets allow access to databases and electronic documents by a defined user group that is generally limited to internal personnel. Intranets may be expanded to include select groups of customers and vendors; such systems are often referred to as extranets.

Security of Internal Networks - The security of internal networks, whether private, local or wide area, needs to be reviewed and evaluated. Internal attacks are potentially the most damaging because an institution's personnel, which can include consultants as well as employees, may have authorized access to critical computer resources. Combined with detailed knowledge relating to the bank's practices and procedures, an internal attacker could access value transfer systems directly, or exploit trusted relationships among networked systems to gain a level of access that allows the attacker to circumvent established security controls. After circumventing the security controls on a value transfer system, the attacker could potentially transfer money or other assets inappropriately.

Security of Public Networks - The use of public networks poses additional risks to those of internal networks. The use of dedicated or leased lines may provide an inappropriate sense of security relating to the confidentiality of data transmitted over public networks. These lines use the infrastructure of public networks; therefore, they are vulnerable to the same attacks as the public networks themselves. Risks include line tapping and the possible interception of transmitted data. In addition, key public network operations and support personnel may be able to access highly sensitive data being transmitted over the networks. Confidential data transmitted via public networks may be intercepted or compromised by individuals for whom the data is not intended. It is therefore prudent to encrypt sensitive data transmitted via public networks.

II. ELECTRONIC CAPABILITIES

Financial institutions have provided electronic capabilities for a number of years. Familiar examples include basic phone banking, automated teller networks, and automated clearinghouse systems. However, technological advances have brought greater sophistication to all users, commercial and retail alike.

For instance, sophisticated phone systems and direct dial-up or Internet computer programs facilitate added access. Traditional products and services can be offered through new delivery channels and entirely new products and services may be developed. For example, aside from promotional, lending, and deposit-gathering activities, banks can support bill payment programs, non-deposit sales activities, and cash management services. Electronic capabilities may also yield new electronic payment options such as digital cash.

Although an over-simplification, electronic capabilities can be segregated into three categories by degree of functionality. The functionality has been defined within three levels. Level I systems can simply provide information as defined by the publisher or allow for transmission of non-sensitive electronic mail (information-only systems); Level II systems can allow users to share sensitive information and communicate (electronic information transfer systems) and Level III systems can facilitate electronic funds transfer and other financial transactions (electronic payment systems). Many systems will involve a combination of these capabilities.

Information-only Systems - Level I

For examination purposes, information-only systems are defined as those which allow access to general purpose marketing and other publicly available information, or the transmission of non-sensitive electronic mail. Examples of such nonsensitive electronic mail may include technical suggestions to the bank's webmaster regarding the bank's web site. In these systems, the publisher (generally, the bank) defines the information to be made available. In this sense, the publisher is simply communicating electronically what has traditionally been made available in print and through other media. The electronic format provides a more cost efficient channel that offers greater flexibility in terms of audience, content, and geography. Management should ensure a program is in place to make the consumer aware that if any electronic mail is sent in this capacity as unencrypted it could potentially be intercepted and/or altered.

Although these sites are generally marketing oriented, each can contain as little or as much information as the publisher desires, and can be linked to other sites that provide additional information. Web sites can also enhance marketing efforts by collecting information about each visitor to a site. This can include user identity, access devices or servers used, and the specific products and services reviewed. With current technology, the type and amount of data collected might be used to target frequent visitors with specific products, services, and information for which the user has shown a previous interest. Management can use this knowledge to target and/or cross-sell products or services to customers identified through electronic means.

Electronic Information Transfer Systems - Level II

Electronic information transfer systems are interactive in that they provide the ability to transmit sensitive messages, documents, or files between financial institutions and users. This category includes electronic mail capability that allows for sensitive messages or confidential information to be sent between the financial institution and the user. It also includes systems in which data or files may be uploaded and downloaded between users and the financial institution's proprietary databases or networks. A bank web site that allows a customer to submit an online loan or deposit account application is an example of an electronic information transfer system.

Communication security is a vital component of information transfer in a networked environment. For instance, the Internet is inherently insecure as information travels openly over a series of connected networks. Communication and system security risks include: data privacy and confidentiality; data integrity; authentication; non-repudiation; and access control/system design. In order to manage the aforementioned security risks, a combination of interrelated technologies, standards, and controls may be employed such as encryption, digital signatures, and certificate authorities.

Fully Transactional Information Systems - Level III

For examination purposes, these systems provide the capabilities of both information-only systems, electronic information transfer systems as well as online, account queries, transfer of funds among accounts, bill payments, and other transactional banking services. These capabilities typically are provided by interactive connectivity between the customer's computer or other device and the bank's internal network or data base. Therefore, this level represents the highest degree of functionality.

Electronic Payment Systems

Electronic payment systems resemble traditional systems because both are derived from a common monetary model. In this sense, electronic systems are simply alternative means to deliver traditional banking and related products and services. Both must complete the same general steps within the payment cycle to reach finality: payment entry, settlement, and distribution. In all cases, trust in the participants (i.e., banks and non-banks that issue, process and settle payments) and confidence in the process are crucial to a particular system's acceptance and survival. These factors have historically maintained the banking industry's central position within the payment system.

Beyond trust and confidence, users evaluate payment systems on a number of criteria, including:

- User privacy;
- Transaction legitimacy, security, and non-repudiation;

- System dependability, efficiency, and cost; and
- Merchant acceptance and convenience.

Electronic payment systems can be broadly categorized according to system components, process methodology, and system structure. The combination of attributes will determine, to a large degree, the amount of risk inherent in a particular system. However, risk will also vary significantly depending on system implementation, administration, and the controls employed by each participant. The following table details various electronic payment system characteristics.

CHARACTERISTICS OF ELECTRONIC PAYMENT SYSTEMS	
System Components:	<ul style="list-style-type: none"> Chip versus magnetic strip technology Card versus computer-based systems System hardware (i.e., PC, card reader, ATM, etc.)
Process Methodology:	<ul style="list-style-type: none"> Batch versus real-time processing Online versus offline access
System Structure:	<ul style="list-style-type: none"> Legal currency versus branded (proprietary) value Single versus multiple currency Debit- versus credit-based systems Open versus closed systems * Reloadable versus single use systems Controlled versus secured access Single versus multiple purpose Integrated versus stand alone systems User anonymity Payment mechanics (buyer and seller interaction) Payment system settlement (processing) Transaction size (micro or large-dollar payments) Geographic reach
<p>* With respect to payment systems, open systems are characterized by broad geographic presence and acceptance by a large number of merchants or programs. Closed systems generally involve a smaller geographic presence and/or a single or limited purpose use.</p> <p>Note: The table is intended to show the primary decision areas in developing a payment system. Software is not specifically included because it converts the decisions regarding components, methodology, and structure into an operative system. Indirectly, software decisions are embedded throughout the table.</p> <p>Note: The subcategorizations do not necessarily present “either... or...” decisions. In many ways, the decisions run along a continuum, such as the degree of security or system integration. Technology also allows for systems to be accessed via multiple media devices and/or channels, such as electronic kiosks, PC dial-up programs and Internet services.</p>	

Bank Roles in Electronic Payment Systems

Participants in an electronic payment system may include users, financial institutions, third party processors, and government-backed central banks. Although electronic capabilities have changed the framework of payment systems, financial institutions will continue to participate in a variety of roles. While financial institutions are familiar with many of the roles, the dynamic environment presents a new set of challenges and risks in nearly every case. Banks may perform any one of the roles described below or a combination of multiple roles.

- **Owner or Investor** - Banks might acquire equity or similar stakes in payment systems, which can take the form of an equity investment, partnership or joint venture arrangement, or consortium member. As such, the bank may bear financial, strategic, compliance, and reputation risks depending on the ownership structure and the venture's success or failure.
- **System Developer** - System development might be undertaken as an in-house effort or under agreements with other parties. In either case, development efforts introduce financial, systemic, reputation, and strategic risks. Potential liability can be well beyond the amount funded, contracted, or, in the case of stored value programs, the amounts held.
- **Issuer** - Issuers sell stored value to participants, either directly or indirectly through another entity. Issuers bear transaction and liquidity risks associated with funding the recorded obligations. Issuers also bear strategic, compliance, and reputation risks, and are potentially liable in the event value is counterfeited or compromised.
- **Distributor/Redeemer** - These roles support stored value systems by distributing or redeeming value. The responsibilities can be taken on individually or can be combined in a dual capacity. In the case of distributing banks, the risks include transaction, compliance, reputation, credit, and liquidity risks. Redeeming banks are exposed to transaction and credit risks.
- **Transaction Authorizer and Processor** - This role is similar to credit card arrangements whereby transactions are authorized through the payment system prior to completion. Responsibilities can include authorizing, remitting, clearing, and settling transactions. Risk areas, which can include credit and liquidity, may be mitigated by adequate operating procedures throughout the transaction process.
- **Recordkeeper/Transaction Archiver** - Although appearing to be largely administrative, these roles maintain audit trails and provide the means to settle disputes among participants. Ineffective operations may result in heightened transaction, reputation, and compliance risks.

- **Trusted Third Party** - In the role of a trusted third party, a financial institution may serve as a certifier for electronic transactions. In this capacity, the bank certifies the identity of one or more parties to an electronic transaction who seek to authenticate each other. Errors or omissions could result in significant liability.
- **Other** - Because many systems are credit or debit based, banks may also serve in traditional roles. These might include providing data processing services much like traditional credit and debit card programs, or serving as a depository and administering funds under the direction of the end user or system provider.

Note: The scope of the safety and soundness electronic banking examination procedures focuses primarily on retail electronic payment systems. Large dollar and wholesale payment systems are addressed in more detail in the FFIEC Information Systems Examination Handbook.

III. RISKS

Regardless of the level of sophistication, risks are inherent in all electronic capabilities. For instance, an information-only web site used for advertising purposes may be inappropriately altered by unauthorized parties. Electronic mail containing confidential or proprietary information may be distributed in error. Networked systems that are directly connected to a bank's central operating system or main database might be accessed by unauthorized parties, revealing sensitive data or applications. System failures have also occurred due to power outages and system defects.

Electronic delivery and payment systems involve a wide range of potential risk exposures. The use of an electronic channel to deliver products and services introduces unique risks due to the increased speed at which systems operate and the broad access in terms of geography, user group, applications, databases, and peripheral systems. In addition to the unique risks, traditional risks which are similar to those in customary banking activities are also present. For example, if a bank conducts lending or deposit gathering activities over an electronic channel, credit and liquidity risks must be considered in the context of the high-speed, global electronic environment.

Specific Risks to Electronic Systems

Unique risks posed by electronic delivery channels are reflected in each of the six areas of concern identified in the following table. While not all-inclusive, the specific risks allude to the rapid transaction speed and broad access associated with electronic delivery channels. Reliance on third party vendors for technology and uncertainties in the legal and regulatory environment also introduce unique risks to electronic delivery and payment systems.

SUMMARY OF SPECIFIC RISKS Electronic Delivery and Payment Systems	
Area of Concern*	Specific Risks and Concerns
Planning and Deployment	<p>Inadequate decision processes while considering, planning, and implementing electronic capabilities</p> <p>Impact of technology cost and pricing decisions on financial position</p> <p>Strategic implications of interstate and global activities</p> <p>System design and capabilities may not meet customer demands</p> <p>Implications of increasing competition from/involvement with non-financial entities</p> <p>Uncertain applicability of blanket bond/other insurance coverages to electronic activities</p>
Operating Policies and Procedures	<p>Managerial or technical incompetence relative to electronic activities</p> <p>Existing controls may not adequately protect confidential electronic information</p> <p>Existing policies and procedures may not address the transaction speed and broad reach of electronic channels</p>
Audit	<p>Audit trails may be lacking in electronic systems</p>
Legal and Regulatory	<p>Uncertain enforceability of digital contracts, agreements, and signatures</p> <p>User privacy issues</p> <p>Contingent liabilities may result from user or participant claims</p> <p>Uncertain legal jurisdiction with respect to taxation, criminal, and civil laws</p> <p>Implications for interstate and international commerce</p> <p>Uncertain regulatory environment (local, national, and international; financial services and other areas)</p> <p>Uncertain applicability of reserve requirements to electronic money</p> <p>Uncertain applicability of financial recordkeeping, disclosure, and other requirements</p> <p>Uncertain acceptability of electronic documentation/disclosures under various regulations</p>
Administration and System Operations	<p>Hardware and/or software failures or disruptions</p> <p>System and/or data base compromise</p> <p>Inadequate system capacity</p> <p>System obsolescence</p> <p>Administration of multiple standards and protocols</p> <p>Inadequate protection of electronic communications</p> <p>Inadequate system security and controls</p>
Vendors and Outsourcing	<p>Reliance on vendor competence to perform critical functions</p> <p>Internal controls may not extend to third party vendors</p> <p>Weak system support among vendor group</p> <p>Maintenance and administration of multiple inter-related systems, activities</p> <p>Failure to monitor inter-relationships among multiple financial institutions, vendors or originators, and participants within a payment system</p>
<p>* These Areas of Concern are generally consistent with the six Review Areas of the Safety and Soundness Electronic Banking Examination Procedures.</p>	

The table identifies numerous risks; however, the threat of failure or compromise in any system is significantly more pronounced in an environment of interconnected computer systems. As such, it is deserving of particular attention. Potential causes of a system compromise include natural disasters, participant failure, or system attacks which are described more fully below:

- **Natural disasters** - The risks presented by natural disasters grow as the geographic reach of a network expands. For instance, the server equipment for a particular system might be distantly located, requiring public telecommunications networks for access. An interruption at any point along the connection might impact service.
- **System attacks** - Internal or external attacks may be undertaken to deny service to others, access databases, manipulate applications, or alter financial outcomes. Beyond financial gain, motives can range from simply trying to overcome system security (the challenge) to commercial espionage. Many perpetrators attempt to hide evidence of the attack, making it more difficult to identify the source or methods employed.
- **Participant failure** - The failure of one or more participants in a payment system can have a significant financial impact on all participants. For instance, membership contracts may require that all participants share in the financial loss from an individual failure. In a worst-case scenario, a significant individual failure might cause other participants, and the entire system, to fail. Because trust and confidence are critical, public reaction to a minor failure could jeopardize an entire system.

The effects of a system failure or compromise can rapidly extend beyond the interested parties. Further, the reputational harm and lost confidence could seriously jeopardize the viability of the underlying system. Comprehensive risk management programs are critical to identifying and responding to any incident.

IV. RISK MANAGEMENT

Traditional risk management programs will need to be adapted to address new aspects of an electronic environment which may include transaction speed, geographic reach, and user anonymity. Such aspects introduce new challenges for management systems designed to monitor activities or trends. For example, questionable activities conducted electronically might not be discovered by traditional review and audit processes. This could limit or distort the quality of information upon which management relies to make effective decisions.

Risk management is the ongoing process of identifying, measuring, monitoring, and managing potential risk exposure. With respect to electronic delivery and payment systems, the process should encompass all significant operational, legal, and reputational risk areas. Depending on the level of activity, consideration may be given to:

- General supervision, as evidenced by: planning and analysis, policies and procedures, accountability and authority, regulatory compliance and legal framework, human resources, and audit;
- Transaction processing, as seen in: user authentication, information integrity, non-repudiation of transactions, and data confidentiality; and
- Systems administration, as evidenced by: resource requirements, system security, system reliability and contingency planning, system capacity, outsourcing policies, and systems update control.

The results of the risk management process should generally be integrated into:

- Strategic planning and feasibility analysis;
- Management supervision and internal controls;
- Operating policies and procedures;
- System administration, audit and testing;
- Physical, transaction and system security;
- Vendor due diligence, and vendor/internal support teams;
- Incident response and preparedness plans;
- Disaster recovery, business resumption and contingency plans; and
- Ongoing review of technological developments and capability enhancements.

The above list is generally comprised of traditional risk management techniques that may be applied to electronic delivery and payment systems. However, risk management techniques which have specific relevance for electronic banking are worthy of further discussion. These include strategic planning and feasibility analysis, incident response and preparedness, and internal controls.

Many institutions outsource the electronic delivery and payment systems in part and/or in whole to third party vendors. However, the bank's board of directors has ultimate responsibility for the bank's system, vendor management, oversight of electronic mail, and all other matters pertaining to the outsourcing arrangement.

Strategic Planning and Feasibility Analysis

As noted above, strategic planning and feasibility analysis should be included in any risk management effort. However, their importance cannot be overstated in moving toward an electronic environment due to the significant investment, opportunities, and risks involved in deploying electronic capabilities. Strategic planning is an ongoing process from which an organization's mission and objectives are developed. Although the processes are similar, the focus of strategic planning is on the organization while feasibility analysis concentrates on specific proposals.

Feasibility analysis is the process of determining the likelihood that a proposal will fulfill specified objectives. The analysis should begin at the point an opportunity is identified, and continue through deployment. Specifically, each opportunity should be analyzed in three stages: (1) Study, during which needs and objectives are analyzed, and alternatives are developed based on performance specifications; (2) Design and Development, during which the best solution is identified based on technical specifications, the system is installed, policies and procedures are developed, and documentation is completed; and (3) Operation, during which the system is operated and maintained.

Once deployed, each system must be subject to ongoing reviews to evaluate performance against current strategic plans and objectives, operating requirements, and technological developments. Any deficiencies should be documented for appropriate action.

Incident Response and Preparedness

A primary focus of risk management is to minimize the negative effects of a problem situation. This can be particularly difficult in an electronic environment that offers speed, sophistication, and access to many users. A user's identity need not be revealed and no relationship is necessary to access bank web sites as these sites are public domains. The nature of this system allows anonymous access by users who may have illegitimate/malicious intent in accessing these systems. Further, because systems may be interdependent, a single problem can have an impact on several areas including product management, marketing and customer service, and operations.

For instance, electronic advertising can provide information about products, services, rates, and fees. Incorrect information can possibly lead to customer complaints, contingent liabilities, or lost opportunities and income. As a result of a system attack, content may be altered to include inappropriate or even objectional material that can be viewed by the general public. Because of inadequate controls and security, users may be able to access, disclose, or improperly use confidential information.

Although the degree of sophistication will vary depending on the risks inherent in each system deployed, establishing an incident response team or preparedness plan provides a platform from which an institution can respond to a problem situation. Just as in contingency planning, the objective is to identify and prepare officers and employees who represent key departments and functions, and who collectively provide the expertise necessary to respond quickly and decisively. The composition of a response team or extent of a preparedness plan will depend upon the level and complexity of electronic banking activity and the institution's available resources.

In assembling a response team or developing a preparedness plan, decisions should be guided by management's judgement. The beginning point is to assess the risks posed by each system deployed to identify the principal departments, resources, activities, and constituencies

potentially impacted by a problem. Individual(s) should then be formally appointed and empowered with the latitude and authority to respond during an incident.

Internal Routines and Controls

Any component of a computer system can be compromised by a number of threats, natural and otherwise. Because threats expand as access to a network expands, the system becomes more vulnerable. However, this vulnerability can be reduced by employing a range of controls that, in combination, protect the operating system and data.

An effective security program does not rely on one solution, but on several measures that, together, serve to identify, monitor, control, and prevent potential risks. The most effective control programs will customize hardware, software, and manual controls during the system development phase.

System controls are an integral part of any risk management program. The extent of such a program should be commensurate with the level and complexity of the activity. Through comprehensive system reviews and tests, controls should be incorporated to protect hardware and software, proprietary data, and electronic transmissions. To ensure maximum effectiveness, management must also recognize the importance of educating all users on the need to adhere to the control standards. This educational effort should also address the risks of not adhering to the standards.

Although not all-inclusive, the table below presents potential risks and mitigating controls that should be considered in developing a system security program.

Potential Risk	Mitigating Controls
<p><u>Unauthorized Intruder Accessing Information</u> System security compromised as a result of a hacker accessing the system, intercepting data during transmission, or wire tapping.</p>	<p><u>Access Control</u> Implement physical and system access controls, including on-site security, system passwords, firewalls, encryption, and intruder detection mechanisms.</p>
<p><u>Loss of Data Integrity</u> Accuracy and reliability of data compromised as a result of unauthorized fabrication, poor audit trails, absent physical signatures, errors introduced into the system, or corruption.</p>	<p><u>Authentication</u> Utilize authentication controls to preserve the integrity of the data. Such controls include acknowledgment, computerized logs, digital signatures, edit checks, and separation of duties.</p>
<p><u>Lack of Transaction Completeness and Inability to Transmit Transactions</u> Loss of transactions during transmission, duplication of transactions due to retransmission, or inability to transmit transactions.</p>	<p><u>Acknowledgment</u> Require acknowledgment controls (batch totaling, sequential numbering, one-for-one checking against the control file), adherence to protocols, anti-virus software, offsite backup, and contingency planning.</p>

Other Considerations

Although consumer protection and other specialized activities are addressed through separate examination programs, weaknesses in these areas can have a significant impact on a bank's overall condition. As such, it is important that plans to deploy electronic systems consider the full range of implications. To do otherwise may impact the institution's compliance posture, and possibly result in consumer complaints or contingent liabilities through civil actions.

V. EXAMINATION PROGRAM

General

The electronic environment continues to evolve in terms of the technology employed and activities conducted. The rapid pace of change in the networked environment calls for a risk management approach to examinations. Therefore, examiners will evaluate an institution's overall effectiveness in controlling the broad risks inherent in electronic delivery systems.

In many cases, financial institutions will deploy multiple systems to provide customers with a range of options. Examiners should complete the safety and soundness electronic banking examination procedures for each system deployed. In this regard, examiners should make a determination as to what level is appropriate for each system. While systems will generally be reviewed individually, consideration should be given to the degree of integration. Examiners should use judgement in identifying common review points, such as operating policies, strategic plans, and identifying how electronic payment systems may be linked together.

The safety and soundness electronic banking examination procedures are intended to compliment traditional examination procedures in the evaluation of specific activities, such as lending, deposit-gathering, and non-deposit activities. Therefore, efforts should be made to coordinate reviews of written policies, internal controls, and other related functions.

Pre-examination Planning

Pre-examination planning should identify electronic banking activities. For example, information requests should be included in the pre-examination letter or addressed during the initial meeting with bank management. Examiners should review information available from the electronic banking data entry system and the bank's web site, if any, to determine the extent and complexity of electronic banking activities.

Examination Levels

Three levels of examination review have been established to recognize the range of risks in electronic systems. The levels are designed to build on one another, such that examiners will complete Level I procedures for all system reviews. In the case of very simple systems such as

those that only provide information to users, the examiner will complete only Level I procedures. In the case of more advanced systems which permit transfer of information or data, examiners will complete Level I **and** Level II procedures. For systems that involve transactional capabilities, **all three levels** will be completed. In those instances in which it is difficult to discern what level should be completed, examiners should consult with information systems specialists. However, as a general rule, examiners should use the higher level procedures in cases of uncertainty.

- **Information-only Systems - Level I** - In the review of very simple systems, only Level I procedures will be completed. Examples of less sophisticated systems include information-only web sites that are limited to presenting electronic versions of marketing or informational brochures, and advertising of products, services, rates, and fees. These systems may also allow the exchange of non-sensitive electronic mail. Since Level I procedures will also be completed for more complex systems, they are designed to be interpreted broadly and examiners should use judgement in applying them to systems having different degrees of sophistication.
- **Electronic Information Transfer Systems - Level II** - These procedures are intended to expand on Level I. Level II procedures should be performed for systems that are capable of accessing and transferring data, files, or messages. This might be through systems that provide uploading and downloading capabilities, or the exchange of electronic messages that contain sensitive or confidential information. Systems that permit the transfer of potentially confidential data will be subject to a Level II review due to the sensitive nature of the information conveyed. Examples of Level II systems include web sites that offer online loan and deposit gathering applications that may be completed online and transmitted electronically.
- **Fully Transactional Information Systems - Level III** - These procedures are intended to expand on Levels I and II. Level III procedures should be performed for systems that enable users to direct or process financial transactions (e.g., transactional web sites, transactional PC dial-up, and stored value systems).

Note: Because the three levels of procedures are designed to build on each other, there are certain review areas that do not include specific items for each level. For example, a particular review area may include specific items for Levels I and II, but no additional items for Level III.

Examination Review Areas

The following six review areas are designed to address electronic banking capabilities. A general description of each review area is provided below. Certain activities in the review areas may overlap with other assignments (such as lending or non-deposit activities). Examiners should coordinate these efforts among the examination team.

Planning and Implementation - Because electronic banking systems facilitate broader access to confidential or proprietary information systems, it is imperative that management (including the board, senior management, and line officers) is fully informed of the opportunities and risks in system deployment. Deficiencies in planning and deployment significantly increase the risk posed to an institution and significantly decrease the ability to respond in a satisfactory manner.

Boards of directors have ultimate responsibility for the electronic systems employed and, accordingly, they should approve the overall business and technology strategies including the bank's risk analysis, feasibility study, and the strategic plan. Senior management should take the necessary steps to provide direction in meeting the necessary security measures regarding electronic banking platforms.

Operating Policies and Procedures - Electronic capabilities can significantly change the character of a bank's business or enable it to introduce new products, services, and delivery channels. Policies, procedures, and other operating guidelines must keep pace with this new environment, either through updates of existing documents or adopting new standards when appropriate.

Segregation of duties is another fundamental element of a sound risk management and internal control system. Failure to implement and maintain such a system with respect to business activities and information security administration, including maintenance of individual security profiles, constitutes a potentially dangerous practice that may lead to a compromise of system integrity.

As discussed earlier, management needs to incorporate or address electronic banking in the institution's overall risk management program. Policies and procedures relating to risk management should also address security concerns. An effective security program depends on the implementation of sound policies, procedures, practices, as well as support from the institution's board of directors and senior management. Several processes need to be evaluated by the institution's management in formulating and maintaining an effective security program. Listed below are some of the areas that should be addressed:

- **Risk Assessment** - inventory systems, applications and data sources. Assess critical and sensitive matters. Evaluate information for the level of protection required (data classification or scoring).
- **Framework** - develop and coordinate policies, procedures, and practices. Address in the institution's overall security program.
- **Delegation** - assign individual authority, responsibility, and accountability to each employee.
- **Training and Development** - educate both employees and customers about the institution's use of electronic platforms.

Audit - An institution's internal control structure is critical to the safe and sound functioning of the organization. A secure operating environment requires an effective system of controls to prevent, detect, and correct information security breaches. In order to achieve this process both audit and segregation of duties need to be in place. Audit procedures are most effective when designed into each system during the development phase. When coupled with a strong risk management program, a comprehensive, ongoing audit program allows the institution to protect its interests as well as those of its customers and other participants. In developing audit programs, the institution must consider the full scope of each application to protect financial and informational assets, system reliability, and user confidence.

Legal and Regulatory Matters - Deploying electronic capabilities necessitates that an institution review the legal and regulatory framework within which each activity will be conducted. Determining that each system meets minimum standards for initiating, completing, and enforcing legal documents and financial transactions protects the value and efficiencies in more sophisticated systems. Failing to review the regulatory standards and legal foundations introduces heightened risk of direct financial loss, regulatory action, or contingent liabilities resulting from civil actions. Whether an advertising medium or a transactional facility, all systems must also be reviewed for compliance with consumer protection requirements.

Administration - Whether electronic capabilities are developed in-house or acquired through a service provider, the bank retains the obligation to ensure minimum standards of operation. Therefore, guidelines such as access levels, exception reporting, and record retention must be established and monitored on a regular basis. Failing to do so might result in a system that cannot operate in the manner anticipated. Depending on the scope of activities, users may be placed at risk due to inadequate security measures or unreliable operations.

An important factor in achieving customer acceptance and confidence involves providing education and support to participants and responding to problem situations. Management should periodically test the system's capacity, availability, and integrity in order to determine that the system can perform and achieve the results intended/promised. Failing to provide reasonable support weakens the user's commitment to the system, increases administrative costs due to avoidable errors, and raises the risk of complaints and legal actions. Risk also increases when a bank fails to inform customers of the security precautions (such as confidential PINs) that users are expected to adopt.

Vendors and Outsourcing - The level of sophistication and the rate of change in electronic capabilities may require at least some degree of outsourcing to third parties. However, this delegation does not lessen the burden on management to supervise and control all aspects of the bank's systems. Delegation through outsourcing requires reasonable due diligence efforts throughout the term of the engagement. Conditions, rights, and responsibilities should be governed by written agreements. This is particularly important because in an electronic environment, short-term engagements, new developments, and untested entities are not uncommon. Further, all outsourcing arrangements must be coordinated to ensure that security, reliability, and integrity are not compromised.

Report Treatment

Examination findings will generally be incorporated into the Risk Management section of the safety and soundness report. Unless otherwise instructed, findings should be addressed collectively as an “other matter.” At a minimum, a brief summary comment describing the bank’s activities should be included. Significant findings should be carried forward to the Management page and Examination Conclusions and Comments page, as per report instructions.

Impact on Bank Ratings

Findings will primarily be factored into the management component rating for safety and soundness examinations. However, this is not to say that other component ratings cannot be materially impacted. The degree of any impact will consider a number of factors, including:

- The specific issues in relation to the volume and trends in transactions, dollars, and customers;
- The apparent risk to the bank’s financial and informational assets, including customer data, regardless of the volume and trends in activity;
- Anticipated growth in volume, whether dollars, transactions, or customers; and
- Anticipated expansion of products, services, or platforms.

Referrals to Specialists

Electronic banking activities impact other examination programs (e.g., information systems, consumer protection, and trust) in addition to safety and soundness. Therefore, contact with specialists in these areas may be necessary to comprehensively evaluate a bank’s activities. Consultations with information systems specialists and electronic banking subject matter experts have been incorporated into the safety and soundness electronic banking procedures at critical junctures. Referrals to compliance and other specialists should be considered with respect to the bank’s activities and the nature of examination findings.

The safety and soundness electronic banking examination procedures encompass traditional control mechanisms such as policies, procedures, and planning. However, examiners are reminded that access and speed can magnify risk in an electronic environment. This is particularly true if risk management programs are ineffective or if a system is linked to a bank’s operating system and databases. In other words, a bank can be exposed to significant risk even if activity volume is nominal. Therefore, varying degrees of contact with information systems specialists and electronic banking subject matter experts will be needed when examining electronic banking activities.

Safety and soundness electronic banking procedures are to be completed for all three levels of review by the safety and soundness examiner. In the case of a Level I examination, an information system specialist should be contacted during the examination in the event that a system is directly connected to the bank's operating system. The Level II procedures incorporate consultation with a specialist when the safety and soundness procedures are completed. This is to solicit input before the findings are finalized and to determine whether a technical review is warranted. The Level III procedures require that a specialist complete a technical examination in addition to the safety and soundness program completed by the safety and soundness examiner. However, in any situation where significant deficiencies or weaknesses are noted, a specialist should be consulted.

Examination plans should consider these needs so that consultations and technical reviews can be completed during the examination. When consultations or technical reviews are delayed due to other demands placed on specialists, examiners should contact the field office supervisor or regional office electronic banking contact for direction.

Electronic Banking Online Data Entry System

Deployment of electronic banking activities does not require a formal application or notification to bank regulators at this time. As a result, it is likely that examiners will identify such activities either during pre-planning activities or during the course of an examination, whether safety and soundness, information systems, consumer protection, or other specialty areas. To effectively monitor bank activities and respond to trends or potential problems, examiners will utilize the online Data Entry System to capture and monitor basic information regarding a bank's activities. The online system will compile and store statistical data in a comprehensive data base.

The Data Entry System should be used at each examination to record the bank's current electronic banking activities and future plans. Field office supervisors should use this information to determine what, if any, follow-up activities are warranted. Such actions might include assigning specialists to the examination underway, scheduling a subsequent visitation, or directing that electronic banking activities be specifically addressed during the next regularly scheduled examination.

Examination Workpapers

Copies of bank documents and other information should support the examination findings and be retained for future reference. Depending on the level of review and complexity of the activity, workpapers may include:

- Summaries of strategic plans, feasibility studies, test results, and other reviews; Flow charts detailing the basic systems deployed in relation to the bank's databases and operating systems;
- Details regarding outsourcing arrangements with third party servicers, including copies of the underlying agreements, third party audits and other reviews;

- Details of any independent reviews or certifications of web sites;
- Information detailing activities conducted, the bank's roles, and delivery channels;
- Standard customer and user agreements;
- Details regarding complaints and lawsuits specific to electronic delivery systems;
- Internal and external audit reports and related materials;
- Summary of disaster recovery and contingency plans; and
- Summaries of relevant operating policies and procedures.

When a bank lacks relevant documentation or information, it may be indicative of management weaknesses in deploying electronic capabilities. Examiners should discuss any apparent deficiencies with bank management.

Electronic Banking

Evaluate the above-captioned function against the following control and performance standards. The Standards represent control and performance objectives to ensure the bank operates in a safe and sound manner and that the entity's objectives are carried out. Associated Risks represent potential threats to the bank if the standards are not achieved and maintained. The Standards are intended to assist examiners in analyzing important functions that may warrant additional review. All of the following Standards may **NOT** need to be considered at every bank. Conversely, these do **NOT** represent all of the control and performance standards needed for every bank. Examiners should continue to use their judgement when assessing risk.

STANDARDS	ASSOCIATED RISKS
MANAGEMENT AND CONTROL	
<p>The board or an appropriate committee approves each of the electronic systems based on a written strategic plan and risk analysis commensurate with the activity.</p>	<p>Systems may be used without clear strategic direction or without a comprehensive risk management program.</p> <p>System design and capabilities may not meet customer demands.</p> <p>Participation of critical business units in the planning process may be omitted.</p> <p>Management may not have considered the impact of technological costs and pricing decisions on the bank's financial position.</p>
<p>The board and management review policies and procedures and make appropriate revisions to incorporate alternative delivery and payment systems.</p> <p>Management provides adequate training and retraining of officers and employees on proper controls and potential risks associated with alternative delivery and payment systems.</p>	<p>Policies and procedures may not adequately address the impact on bank activities, operations, or security.</p> <p>Existing controls may not adequately protect confidential electronic information.</p> <p>Poor training may result in managerial or technical weaknesses.</p>
<p>Internal and external audit programs incorporate alternative delivery and payment systems.</p>	<p>Potential weaknesses may not be identified within a specific system or within the total environment of inter-related systems.</p>
<p>Each system or activity is specifically reviewed to establish the legal foundations and address regulatory issues.</p>	<p>Enforceability of digital contracts, agreements, and signatures may be uncertain.</p> <p>Activities/operations may be introduced that are not consistent with regulatory and legal standards.</p> <p>Contingent liabilities may result from user or participant claims.</p>

STANDARDS

ASSOCIATED RISKS

The board establishes appropriate standards and procedures for overall program administration and systems operation.

Adequate contingency and disaster plans exist.

Information is secure and the bank's internal system(s) are adequately protected against attack from both internal and external sources.

The bank may have inadequate protection of electronic communications and poor system security and controls.

The system may become obsolete or need to be upgraded as technological developments are introduced into the marketplace.

The system may not have sufficient capacity to meet the bank's and customers' needs.

Poor contingency planning may aggravate or result in hardware and software failures or disruptions.

The bank could be liable to customers for losses due to system interruptions.

Attackers could obtain access to confidential bank or customer information, alter the user interface to contain inappropriate or inaccurate material, introduce viruses into the bank's information system, or cause other damage.

Intrusion attempts may not be detected, contained, and reported in a timely manner.

Unprotected data transmissions could compromise sensitive information.

Lack of control over physical access to system hardware and software.

Appropriate standards are established to administer outsourcing arrangements.

Management may become over-reliant on third party service providers to perform critical functions.

Adequate internal controls may not be initiated by third party vendors.

Management may have difficulty monitoring interrelationships among multiple financial institutions, vendors or originators, and participants within a payment system.

The bank's electronic banking services could be disrupted if vendors or third-party providers are not financially stable.

CORE ANALYSIS

Consider the following procedures at each examination. Examiners are encouraged to exclude items deemed unnecessary. This procedural analysis does not represent every possible action to be taken during an examination. The references are not intended to be all-inclusive and additional guidance may exist. Many of these procedures will address more than one of the Standards and Associated Risks. For the examination process to be successful, examiners must maintain open communication with bank management and discuss relevant concerns as they arise.

IMPORTANT

Electronic capabilities can generally be segregated into three categories by degree of functionality or level of service (Level) provided by the bank. Level I systems can simply provide information as defined by the publisher or allow for transmission of non-sensitive electronic mail (“information-only systems”); Level II systems can allow users to share sensitive information and communicate (“electronic information transfer systems”) and Level III systems can facilitate electronic funds transfer and other financial transactions (“electronic payment systems”). Some banks may use multiple systems that involve different degrees of functionality (Level I, Level II, and Level III).

The Levels are designed to build upon one another, such that examiners will complete Level I procedures for all system reviews. For very simple systems that only provide information and non-sensitive electronic mail to users, the examiner will complete Level I procedures. For more advanced systems that permit the transfer of sensitive information or data, examiners will complete Level I and II procedures. For systems that involve transactional capabilities, examiners will complete Level I, II, and III procedures. In instances where it is difficult to discern what Level to complete, examiners should consult with information systems specialists or subject matter experts (SMEs). However, as a general rule, examiners should use the higher Level procedures in cases of uncertainty.

Examiners are encouraged to seek additional guidance or direction from information systems specialists or subject matter experts regarding electronic banking examination procedures during each examination. **If there is a direct/indirect connection between the bank’s internal operating system(s) and the system that hosts the external electronic service or function, an information systems specialist should be consulted.**

PLANNING AND IMPLEMENTATION

Level I

Determine whether the board, or an appropriate committee, approves each of the electronic systems based on a written strategic plan and risk analysis commensurate with the activity. The analysis should address the following issues:

- The function of electronic delivery channels within the strategic or operating plan.
- Risks associated with each electronic system.

Determine whether management reviews the bank’s defined trade area. *(Note: In the context of these procedures, the bank’s defined trade area is viewed strategically and should not be confused with its delineated community for Community Reinvestment Act purposes.)*

- Determine if guidelines for accepting account applications and other relevant policies and procedures are updated to address activities beyond the traditional trade area.

Ascertain if experienced individuals have been designated to develop and implement electronic banking services, have clearly defined and segregated duties/responsibilities, and have adequate resources to meet their responsibilities.

CORE ANALYSIS

Determine if each system is adequately tested.

- Volume stress testing (to ensure system capacity).
- Screen testing (to review content).
- Pilot program (to evaluate feasibility).

Determine if management provides adequate training for all officers and staff affected by electronic banking systems, including those responsible for products, services, information systems, audit, compliance, and legal issues. (*Note: The training program should be ongoing.*)

Determine if management has confirmed the applicability of insurance coverage, such as blanket bond and excess liability coverage, errors and omissions, and other coverages. Confirm that any gaps in coverage were appropriately addressed.

Level II

Determine whether management completes or obtains a feasibility study for each system implemented.

- Determine whether the study considers various scenarios, including “worst case” scenarios.
- Determine if senior management and the board review the study.

For each system that interacts with any of the bank’s operating systems or databases, determine whether management requires a review of the interactive components and processes to ensure compatibility and security. (Obtain topology map to determine.)

Determine if management verifies the accuracy and content of financial planning software, calculators, and other interactive programs (between the bank and its customers) available through the systems.

Determine if a backup system or method is established for users to conduct normal activity in the event the system is not available for an extended period of time.

- Determine if instruction guides are available that address the back up system or method.
- Determine if management establishes procedures to notify users in the event of a problem.

Determine if management ensures that physical access to computer hardware, software, communication equipment, and communication lines are restricted to appropriate personnel.

Level III

There are no Level III items for this review area.

OPERATING POLICIES AND PROCEDURES

Level I

Review relevant operating policies and procedures to determine if they are updated for the unique character and principal risks associated with alternative delivery channels (including electronic advertising).

CORE ANALYSIS

- Determine if all applicable policies address any new products, services, or delivery channels impacted by electronic capabilities.

Determine that the bank has an adequate electronic banking security program that addresses the following, as appropriate:

- access to, protection of, and disclosure of, customers' confidential information,
- methods for establishing the legitimacy of each party requesting an account action or submitting related instructions or data,
- what information may be shared with third-parties, and
- the ability of third-party servicers to access or monitor electronic transmissions between the bank and any of its customers.

Level II

Determine if policies and procedures governing access to, and the disclosure of, customers' confidential information are updated for electronic capabilities.

- Determine if the policies address what information may be shared with third parties such as non-deposit product representatives, discount brokerage services, etc.
- Determine if guidelines pertaining to confidential information are included as part of the contracts and agreements covering third party arrangements.

Determine if management establishes policies and procedures that control any third party servicer's (electronic system providers, data processors, etc.) ability to access or monitor electronic transmissions between the bank and any of its customers.

- Determine if these guidelines are included as part of the contracts and agreements covering the service arrangements.

Level III

Determine if customers are required to submit a signed authorization for each payee included in bill payment, funds transfer, and similar programs.

- Determine how the bank verifies the legitimacy of each payee.
- Determine if the bank adopts reasonable guidelines for adding or removing payees.

Determine if procedures are in place to control customer transfers of uncollected funds from each access point.

Confirm that safeguards are in place to detect and prevent duplicate transactions within each system.

Determine if appropriate disclosures are made to customers regarding system security, controls, and liability.

Determine if the bank's periodic reconciliation procedures incorporate the full scope of transactional capabilities. Determine if the procedures apply to the general ledger and subsidiary accounts, as appropriate

CORE ANALYSIS

Determine what reporting mechanisms are used to track the nature, volume, and trends in activity for each system deployed. The reports should include a comparison of actual performance to projections.

Determine if the measurements above are incorporated into strategic and operating plans, budgets, and other analyses. *(The measurements should be incorporated into all relevant operating policies and procedures, such as funds management, liquidity, and interest rate risk.)*

Determine whether appropriate operating policies and procedures are established and updated to address the following issues for customer activities:

- Fund transfers. *(Can customers initiate transactions via Fedwire or other payment systems, and if so, have appropriate policies and safeguards been implemented.)*
- Dollar limits per transaction time period (such as per day limit) and relationship.
- Minimum credit standards for participants, as appropriate.
- Settlement guidelines.
- Daylight overdrafts. *(Determine whether transaction volume has been projected for the services offered, and that the bank has determined that current and planned capacity are appropriate to meet those projections.)*

For systems that permit access to credit lines, determine if draws or credit extensions are adequately controlled.

Determine whether appropriate policies and procedures are established to govern foreign exchange activities, if applicable.

Determine whether the bank's policies regarding separation of duties are updated to recognize the access afforded by electronic capabilities.

AUDIT

Level I

Determine if the bank's internal and external audit programs have been updated to specifically address electronic activities and systems.

- Determine if the audit department is appropriately staffed to cover electronic banking activities and whether the scope and frequency sufficiently covers electronic banking. *(Note: The audit program should consider the full scope of each application to protect financial and informational assets, and system reliability.)*
- Review the most recent audit report for major findings. Assess management's ability to correct deficiencies.

Level II

Determine if appropriate audit trails are incorporated into each system.

Level III

Determine whether the audit trails and procedures cover the flow of transactional activity (from initiation to completion) within the set of systems.

CORE ANALYSIS

LEGAL AND REGULATORY MATTERS

Level I

Determine if management establishes appropriate guidelines and practices to comply with advertising requirements. (For example, FDIC Part 328 regarding advertising of membership.)

Determine if any electronic advertisements for non-deposit investment products include appropriate disclosures.

Level II

Determine if the underlying customer, vendor, and merchant agreements/contracts fully address the rights, responsibilities, and liability for each party.

- Determine if the documents address the bank's authority to monitor, store, and retrieve electronic transmissions (including messages and data) between the bank and its customers.

Determine whether management has considered the applicability of relevant state laws and/or UCC standards addressing digital signatures and related certifications, as applicable.

Determine if outsourcing arrangements with vendors and subcontractors are included in the bank's consumer protection and compliance reviews.

Level III

Determine if appropriate procedures exist to ensure compliance with Financial Record Keeping and Bank Secrecy Act requirements, including Know Your Customer guidelines. (*Procedures should be established to identify potentially structured transactions.*)

For stored value systems, determine whether the underlying agreements covering payment systems reasonably address claims of lost or stolen value among the bank, its customers, and third parties.

ADMINISTRATION

Level I

Determine whether there is a direct/indirect connection between the bank's internal operating system(s) and the system that hosts the external electronic service or activity (for example, a web site). **If there is a direct connection, an information systems specialist should be consulted.**

Determine if a program exists for ongoing reviews of each system for the following areas:

- Content.
- Continued appropriateness.
- Accuracy and integrity.
- Security and controls.
- System updates and obsolescence.
- System capacity.

CORE ANALYSIS

- Strategic direction.

Determine whether appropriate procedures exist for maintaining links with other web sites, including both external and internal sites (intranets or other private networks). (*Management should monitor these linked sites regularly for continued appropriateness and accuracy of the site addresses.*)

Determine if procedures exist to monitor unauthorized attempts to access the bank's system.

- Determine if the bank's policies require formal reporting consistent with Part 353 in the event of attempted or actual attacks against any of the bank's systems.
- Review all known incidents and ensure they were reported to the proper authorities.

Determine whether management established a preparedness plan or an incident response team to handle problem situations. If a team has been established, determine if the board approved a written delegation of the team's responsibilities and authority.

Determine if policies and procedures exist to address the bank's use of electronic mail (internally/externally). Determine if the policies and procedures address the following issues:

- Transmissions among all user groups, including customers, officers, and employees.
- Define permissible content to minimize risk from improper disclosure.

Level II

Determine if senior management establishes appropriate levels of access to information and applications for officers, employees, system vendors, customers, and other users. Determine if the access levels are enforced and reviewed on a regular basis.

Determine how the bank establishes the legitimacy of each party requesting an account action or submitting related instructions or data.

Determine if management establishes appropriate programs for customer service, support, and education. Determine if the following support and control activities exist:

- Appropriate educational and reference materials are made available to customers regarding system security, controls, and liability.
- A program exists to address recurring problems in a timely manner.

Determine if retention guidelines exist and are updated for source documents supporting electronic activities, such as account applications, instructions for account transactions, and other records. Determine whether the guidelines also address electronic mail, data files, and similar records.

Determine if management generates and reviews exception reports on a periodic basis.

Level III

Determine whether the bank offers any guaranty or similar pledge in relation to any payment or delivery system. Determine if such guaranties are reviewed by the bank's legal counsel, as applicable.

CORE ANALYSIS

For any stored value program, ensure management determines whether the underlying funds represent insured deposits.

VENDORS AND OUTSOURCING

Level I

Determine if the bank entered into formal contracts with each vendor. Determine if the contracts contain the following information and are reviewed by bank legal counsel, if appropriate:

- Access, ownership, and control of customer data and other confidential information.
- Reasonable assurances for continuation of service through back up arrangements in the event of a problem situation.
- Subcontractors and other supporting vendors.
- Reasonable control and update of content and capabilities in a timely manner.
- Opportunities to review independent annual audits and similar reports.
- Security precautions on the part of the service provider.

Determine if the expiration dates for inter-related service contracts coincide.

Determine if reasonable requirements exist for periodic due diligence reviews of third party providers, including contractors, subcontractors, support vendors, and other parties.

Level II

Determine if management implements appropriate measures to protect against violating licensing agreements if software is being distributed.

Level III

There are no Level III items for this review area.

NOTES:

CORE ANALYSIS DECISION FACTORS

Evaluate Core Analysis results in this section for significance and to determine if an Expanded Analysis is necessary. Negative responses to Core Analysis Decision Factors may not require proceeding to the Expanded Analysis. Conversely, positive responses to Core Analysis Decision Factors do not preclude examiners from proceeding to the Expanded Analysis if deemed appropriate.

1. Is an effective risk management program in place?
2. Are adequate policies and procedures in effect and enforced?
3. Does the audit program adequately address stand-alone, inter-related, and integrated systems?
4. Are the bank's operations consistent with regulatory requirements?
5. Is program administration and oversight adequate?
6. Is an effective vendor oversight program in effect?

REPORT OF EXAMINATION PRESENTATION

Discuss analysis, conclusions, and recommendations with the EIC; an information system specialist or subject matter expert, if applicable; and management prior to completing the following pages, as necessary.

- Appropriate items on the Risk Management page.
- Management/Administration.

NOTES:

EXPANDED ANALYSIS

Generally, procedures used in this section should target concerns identified in the Core Analysis and Decision Factors. The flexible guidelines specified in the Core Analysis also apply here.

An Expanded Analysis should be performed in situations where systems are more sophisticated or when significant deficiencies exist. The Expanded Analysis involves technical procedures that should be performed by an information systems specialist or subject matter expert.

Contact an information systems specialist or subject matter expert (and FOS, Regional Electronic Banking Contact, or Case Manager, depending on regional procedures) and forward a copy of the completed Core Analysis information to the specialist.

Additional procedures for the Expanded Analysis will be determined by the information system specialist or subject matter expert based on the weaknesses found in the Core Analysis.

Discuss the findings of the Expanded Analysis with the information specialist or subject matter expert and include findings and recommendations in the safety and soundness ROE. *(Note: In certain circumstances, the specialist's findings and recommendations will be provided under separate cover; however, any deficiencies that affect the bank's financial condition should be included in the safety and soundness ROE.)*

If a specialist is not available to complete an Expanded Analysis prior to completing the safety and soundness examination, examiners should inform management and the board that an Expanded Analysis will be conducted in the future.

- Examiners should discuss any findings or deficiencies with electronic banking discovered in the Core Analysis in the ROE, and state that further review will be forthcoming.
- If the weakness identified in the Core Analysis are considered severe, attempt to discuss issues with a specialists or subject matter expert in order to determine the materiality and impact the deficiencies have on the bank's financial condition.

NOTES:

EXPANDED ANALYSIS DECISION FACTORS

The following questions will help to evaluate the significance and materiality of deficiencies or other specific concerns identified in the Core and Expanded Analyses.

1. Are (management/performance) deficiencies immaterial to the bank's condition?
2. Could identified weaknesses in electronic banking negatively/materially impact other CAMELS ratings?

REPORT OF EXAMINATION PRESENTATION

Discuss analysis, conclusions, and recommendations with the EIC and management prior to completing the following pages as needed:

- Those pages listed in the Core Analysis Decision Factor section.
- Examination Conclusions and Comments.
- Matters Requiring Board Attention.

NOTES:

IMPACT ANALYSIS

This section helps to evaluate the impact of deficiencies identified in the Core and Expanded Analyses and Decision Factors on the bank's overall condition. This section also directs the examiner to consider possible supervisory actions.

Determine the impact electronic banking deficiencies have on the bank's financial condition, specifically on capital, earnings, liquidity, asset quality, operational controls, risk management controls, and assess the future impact on the institutions condition. *(Coordinate with information system specialist or subject matter expert.)*

Findings will primarily be factored into the management component rating for safety and soundness examinations. However, findings may also impact other CAMELS ratings. The degree of any impact will consider a number of factors:

- The specific issues in relation to the volume and trends in transactions, dollars, and customers.
- The apparent risk to the bank's financial and informational assets, including customer data, regardless of the volume and trends in activity.
- Anticipated growth in volume of dollars, transactions, or customers.
- Anticipated expansion of products, services, or platforms.

Determine the need for administrative and enforcement actions, formulate specific recommendations, and advise the Field Office Supervisor and the Regional Office on the nature of the supervisory concerns.

REPORT OF EXAMINATION PRESENTATION

Discuss analysis, conclusions, and recommendations with the EIC and management prior to completing the following pages as needed.

- Those pages listed in the Expanded Analysis Decision Factor Section.

NOTES:



Request for Information by the

FEDERAL DEPOSIT INSURANCE CORPORATION

DATE XX, XXXX

Mr/s.(NAME), (TITLE)
The (BANK NAME)
(STREET ADDRESS)
(CITY), (STATE) (ZIP CODE)

Dear (TITLE) (NAME):

A safety and soundness examination of your institution is scheduled to begin on _____. A review of electronic banking will be conducted in the scope of that examination. Assistance on your part prior to the start of the examination will considerably lessen the burden and inconvenience that otherwise might be placed on you and your staff. Therefore, it is respectfully requested that the information described on the attached sheet be furnished to the examination personnel. Replies should be directed to the attention of the Examiner-In-Charge. Please reference all responses to the appropriate question number; if any request is not currently applicable, so state. Any requests for clarification or definition of terms should be directed to the Examiner-in-Charge.

(EIC NAME)
Examiner-in-Charge
(MAILING ADDRESS)
(PHONE NUMBER)
(EMAIL ADDRESS)

Attachments:
Request Items

REQUEST ITEMS: *Please respond only to those request items checked.*

- ___ 1. Please provide the electronic banking contact's name, title, and phone number. In addition, please provide the organizational chart of electronic banking personnel including their job descriptions. (P L1)
- ___ 2. Please list all electronic banking platforms utilized and system topology maps including servers, routers, firewalls, and other supporting system components. (P, A L1; P L2)
- ___ 3. Copy of any risk analysis or reviews of electronic banking activity. (P L1)
- ___ 4. Provide list of pending lawsuit/contingent liabilities with potential losses relating to electronic banking activities. (A L3)
- ___ 5. Provide due diligence reviews of third party providers, contractors, support vendors, or any other parties. (P V L1)
- ___ 6. Provide any system security reviews conducted by third parties. (P V L1)
- ___ 7. Copy of all contracts/agreements with vendors, customers, third-parties, etc. (P, V L1; P, O, L L2)
- ___ 8. Copy of insurance policies covering electronic banking activities such as blanket bond, liability coverage, errors and omissions, and any riders relating to electronic banking activities. (P L1)
- ___ 9. Copy of strategic plan and feasibility studies (cost/benefit analysis), test plans and results, deployment plans and reviews relating to electronic banking activity. (P L1-2)
- ___ 10. Provide any reports that measure or analyze actual performance to projections including performance in strategical areas such as deposit growth and technical areas, such as the ability to process the current level of transactional or support activity. (A L1)
- ___ 11. Copy of general policies relating to electronic banking activity (defining bank's trade area, accepting account applications, compliance with Financial Recordkeeping and BSA requirements, etc.). (P L1; O L2; L L3)
- ___ 12. Copy of specific policies and procedures relating to electronic banking operations for items such as new products, services, or delivery channel - i.e. directly related to specific platforms (for example Internet banking, phone banking, etc.) and applications such as email, bill payment, dollar limits per transaction, settlement guidelines, overdrafts, uncollected funds, reconciliation procedures, disclosures, foreign exchange, among others. (O L1-L3)
- ___ 13. Copy of policies for reporting and responding to electronic banking platform system delays, problems, and log book. (P, A L2)
- ___ 14. Copy of policies or written procedures relating to electronic banking security program. (O, L1)
- ___ 15. Copy of the most recent system reports provide by electronic banking platforms used to track nature, volume, trends, and unauthorized attempts into the bank's system. (A L1-2)
- ___ 16. Copy of audits relating to electronic banking. Provide external auditor's engagement letter and management letter including scope and findings. For internal audit, please provide audit schedule, scope, and auditors resume. (D L1-3)
- ___ 17. List or report of authorized users and levels of access for electronic banking platforms, including officers, employees, system vendors, customers, and other users. (P, A L1-2)
- ___ 18. Copy of exception reports, review of logs, and the name of the employee who reviews subject reports and when. (A L1-2; P L2)
- ___ 19. Copy of the bank's back-up/contingency planning for electronic banking platforms. (A L1; P L2)
- ___ 20. Copy of electronic banking training (for example products, services, informational) schedule with dates, attendees, and topics. Provide copies of any educational material and customer agreements. (P L1; A L2)

NOTE: References are provided next to each request item that indicate which area of review and level the item will be used to address. The following key explains the abbreviations used.

Key:

Planning and Implementation	=P	L1 = Level I
Operating Policies and Procedures	=O	L2 = Level II
Audit	=D	L3 = Level III
Legal and Regulatory	=L	
Administration	=A	
Vendors and Outsourcing	=V	

ELECTRONIC BANKING GLOSSARY

Access Products - products that allow consumers to access traditional payment instruments electronically, generally from remote locations.

Acquirer - in an electronic money system, the entity or entities (typically banks) that hold deposit accounts for merchants and to which transaction data are transmitted.

Alpha Test - the first stage of testing a new software product, carried out by the manufacturer's 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 for Information Interchange (ASCII) - a standard code for representing characters as numbers that 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.

Asynchronous Transfer Mode (ATM) - method of transmitting bits of data one after another with a start bit and a stop bit to mark the beginning and end of each data unit.

Auditability - the degree to which transactions can be traced and audited through a system.

Authentication - 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, they may be authorized different types of access or activity.

Bandwidth - the transmission capacity of a computer channel or communications line.

Bastion Host - a system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack. Bastion hosts are often components of firewalls, or may be “outside” web servers or public access systems.

Baud Rate - measurement of data transfer speed.

Beta Test - the second stage of a new software product that is almost ready for market, carried out by volunteers in a wide variety of settings like those in which the finished product will be used.

Biometrics - a method of verifying an individual’s identity by analyzing a unique physical attribute.

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 permits multimedia (graphics) applications on the World Wide Web.

Bundled Software - software that is sold in combination with hardware.

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.

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 method of allocating resources in a local area network so that computing power is distributed among computer workstations in the network but some shared resources are centralized in a file server.

Closed Network - a telecommunications network that is used for a specific purpose, such as a payment system, and to which access is restricted (also referred to as a private network).

Closed Stored Value System - a system in which value is issued and accepted by either a relatively small group of merchants, or in which the system is limited geographically (i.e., university programs and fare cards for mass transit systems).

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 which contain enormous amounts of useful, specific security information.

Cracker - a computer operator who breaks through a system's security. This can be legitimate activity, such as to test system security measures.

Cryptography - the principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form (i.e., scrambling a message).

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.

Database Administrator (DBA) - the individual with authority to control the data base management system.

Data Encryption Standard (DES) - U.S. government standard for data encryption method published by the National Institute of Standards and Technology for the encryption of sensitive U.S. government data which does not fall under the category of national security related information. The DES uses a 64 bit key.

Data Integrity - the property that data meet with a priority expectation of quality.

Dedicated - assigned to only one function.

Design Phase - the phase during which the problem solution that was selected in the Study Phase is designed. The design includes the allocation of system functions; the design of inputs, outputs, and files; and the identification of system and component requirements.

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.

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 Signatures - 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.

Distributed Transaction Processing - application processing that involves multiple users requiring concurrent access to a single shared resource.

Domain Name - an alpha-numeric name for a web site that includes both the online address and online name.

Double Spending (Re-spending) - creating and spending copies of stored value files.

Download - to transmit a file or program from a central computer to a smaller computer or a remote site.

Electronic Benefits Transfer (EBT) - the electronic delivery of government benefits, using plastic cards and available ATM and point-of-sale (POS) technology.

Electronic Cash - the digital equivalent of dollars and cents (also referred to as digital cash).

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.

E-mail - messages people send to one another electronically from one computer to another.

Encryption (Cryptography) - the process of scrambling data by a device or encoding principle (mathematical algorithms) so that the data cannot be read without the proper codes for unscrambling the data.

End-to-end Encryption - the protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

Ethernet - a type of local area network originally developed by Xerox, communication takes place by means of radio frequency signals carried over coaxial cable.

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.

Flowchart - a programming tool to graphically present a procedure by using symbols to designate the logic of how a problem is solved.

Gamma Test - the third stage of software testing completed before release.

Gateway - a computer that performs protocol conversion between different types of networks or applications.

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 (pictures) and windows with a mouse.

Groupware - software that allows a group of people 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, either for malicious reasons or just to prove it can be done.

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, and links to other hypertext documents.

Hypertext Transfer Protocol (HTTP) - 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.

Incident Response Team - a team of computer experts (internal or external) organized to protect an organization's data, systems, and other assets from attack by hackers, viruses, or other compromise.

Integrated Circuit Card (IC Card) - a plastic card in which one or more integrated circuits are embedded (also called a chip card).

Integrated Services Digital Network (ISDN) - a type of all-digital telephone service. ISDN lines provide a connection that can transmit digital data as well as voice, without a modem.

International Organization for Standardization/Open Systems Interconnection (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 Service Provider (ISP) - an entity that provides access to the Internet and related services, 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.

Issuer - in a stored value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it.

Key - A secret value or code used in an encrypting algorithm known by one or both of the communicating parties.

Large-dollar Funds Transfer System - a funds transfer system through which large-dollar and high-priority funds transfers are made between participants in the system for their own account or on behalf of their customers. Sometimes known as wholesale funds transfer systems.

Limited Purpose Prepaid Card - a prepaid card which can be used for a limited number of well-defined purposes. Its use is often restricted to a number of identified points of sale within a specified location. In the case of single-purpose prepaid cards, the card issuer and the service provider may be identical.

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 System - 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.

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.

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.

Multipurpose Prepaid Card - a prepaid card which can be used for a wide range of purposes and has the potential to be used on a national or international scale but may sometimes be restricted to a certain area.

National Institute for Standards and Technology (NIST) - established within the Department of Commerce to develop technical, management, physical and administrative standards and guidelines for the cost effective security and privacy of sensitive information in Federal computer systems. NIST issues the Federal Information Processing Standards (FIPS).

National Security Agency (NSA) - responsible for government and/or military information security.

National Telecommunications Information Administration (NTIA) - 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.

Newsgroup - public forums or discussion areas on a computer network; generally topic-focused.

Node - any device, including servers and workstations, connected to a network. Also, the point where devices are connected.

Non-repudiable Transactions - transactions that cannot be denied after the fact.

Offline - 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 communicate with a computer network. Connections can be direct (as in a LAN using dedicated connections) or indirect (as in using the Internet).

Online Scrip - debit accounts on the Internet or other major computer network.

Online Service Providers (OSP) - closed network services that provide access to various computer sites or networks for a fee.

Open Network - a telecommunications network to which access is not restricted.

Open Stored Value System - a system that may be comprised of one or more electronic cash issuers of stored value that is accepted by multiple merchants or entities.

Operating System - a program that controls a computer and makes it possible for users to enter and run their own programs.

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.

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.

Personal Identification Number (PIN) - a sequence of digits used to verify the identity of a device holder.

Piggyback (Between-the-lines Entry) - a means of gaining unauthorized access to a system via another user’s legitimate connection.

Point of Sale (POS) - a system of terminals that debits or charges a customer’s account and credits or pays a merchant’s account to effect payment for purchases at retail establishments.

Prepaid Card - a card on which value is stored, and for which the holder has paid the issuer in advance.

Privacy - in the context of a payment system, the property that no information which might permit determination of transactions may be collected without the consent of the counterparties involved.

Privacy Enhanced Mail (PEM) - an Internet standard for secure electronic mail. The standard adds several security services to the Internet electronic mail messages: message origin authentication; message integrity; nonrepudiation of origin; and message confidentiality.

Protocols - a standardized set of rules that define how computers communicate with each other.

Proximity Cards - cards that can be read from a short distance; mainly used for security and vehicle identification.

Public Key Cryptography - type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

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.

Remote Payment - a payment carried out through the sending of payment orders or payment instruments.

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.

Router - a computer system in a network that stores and forwards data packets between local area networks and wide area networks.

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 Electronic Transaction (SET) - a set of standards jointly developed by Visa, MasterCard, and several technologies companies to facilitate secure credit card transactions over the Internet.

Secure Hypertext Transfer Protocol (SHTTP) - provides secure communication mechanisms between an HTTP client-server pair.

Secure Socket Layer (SSL) - a protocol for providing data security during transmission using data encryption, server authentication, and message integrity.

Server - a computer that provides services to another computer (the client).

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 Protocol (SMTP) - 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.

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 via magnetic stripe or computer chip.

Structured Query Language (SQL) - a query language used to manipulate large 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.

System Flowchart - a flowchart diagramming 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 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 generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations when due.

Systems Analysis - the performance, management, and documentation of the four phases of the life cycle of a business system: study, design, development, and operation.

Tamper-evident - the capacity of devices to show evidence of physical attack.

Tamper-proof - the proven capacity of devices to resist all 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 via 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.

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).

Transferability - in electronic money systems, the degree to which an electronic balance can be transferred between devices without interaction with a central authority.

Transport Control Protocol/Internet Protocol (TCP/IP) - a standard format for transmitting data in packets from one computer to another, on the Internet and within other networks. TCP deals with the construction of the data packets while IP routes them from machine to machine.

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 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.

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 newsgroups distributed via the Internet.

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.

Web Page - a screen of information supporting the home page of a web site.

Web Site - the collection of an entity's home page and other proprietary pages located on the World Wide Web.

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.

World Wide Web (web, www) - a subnetwork of the Internet through which information is exchanged via 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.