of Terminology . . .

A

Access - The ability to physically or logically enter or make use of an IT system or area (secured or unsecured). Access is the process of interacting with a system.

Access control – Controls that limit or detect access to computer resources (data, programs, equipment, technology, and facilities) and protect against unauthorized modification, loss, and disclosure.

Accreditation - A formal acceptance of risks by management that results from the operation of an information system.

ACH - Automated Clearing House. The ACH is the primary system that agencies use for electronic funds transfer. The ACH Network uses batch processing and a store-and-forward system – moving billions and trillions of electronic financial transactions each year. For many years, NACHA has been the trustee of the ACH Network – employing a collaborative, self-regulatory model to facilitate expansion and diversification of electronic ACH payments (see "NACHA").

Administrator privileges - Computer system access to resources that are unavailable to most users. Administrator privileges permit execution of actions that would otherwise be restricted.

Agency - A legal relationship between two parties who agree that one (the agent) is to act on behalf of another (the principal), subject to the latter's general control. The principal generally is held liable for the agent's actions.

Agility - In IT systems, the ability to rapidly incorporate new technologies or changes to technologies allowing an organization to adapt to changing business needs.

Air-gapped environment - Security measure that isolates a secure network from unsecure networks physically, electrically, and electromagnetically.

Anomalous activity - The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.

Antivirus/anti-malware software - A program that monitors a computer or network to identify all types of malware and prevent or contain malware incidents.

Application security - Measures taken and applied to software (i.e., source code) throughout its life cycle. Application security prevents gaps in the security policy of an application or an underpinning system through application flaws or vulnerabilities in its System Development Life Cycle.

Application development - The process of designing and building code to create a computer program (software) used for a particular type of job.

Asset - In computer security, asset is a major application, general-support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically-related group of systems.

Asset Inventory – An organization or agency establishes an inventory baseline by identifying and recording important information about assets, such as their location, license information, and security classification or categorization. Asset management is the effective placement of data into categories. The

placement ensures that movement of assets and changes to its information are documented, supported, and maintained throughout the asset inventory life cycle.

Asset Ownership – Every asset has an assigned owner and may be an individual or a role. For example, an asset owner of computer hardware may be an IT Director, Manager, or Officer. The designation as an "owner" usually means that the individual or party is responsible for the security of the asset and assigns ultimate accountability.

Asset Use and Acceptability – Acceptable use of assets is established and maintained as a policy comprised of rules and responsibilities of asset usage. There are internal and external parties, which are in accordance with the security classification of each asset. In some cases, groups of assets with similar categorizations may be covered by a similar policy. Yet, all asset categorization, use, and acceptability are endorsed by senior management and/or organizational leadership.

Asset Type: Data/Information – Databases, personnel records, proposals, contracts, SLAs, procedures, policies, manuals, statistics, and any data/information in either hard copy or soft form.

Asset Type: Hardware – Computer/network equipment including tapes, disks, and removable media.

Asset Type: Intangible – Reputation, image, influence, and intellectual property.

Asset Type: People – Staff with expertise, skill, and knowledge of a subject.

Asset Type: Service – Electricity, telecommunication, facility plant management, and technology.

Asset Type: Software – Application software, system software, system utilities, and development tools.

Attack signature - A specific sequence of events indicative of an unauthorized access attempt.

Authentication - The process of verifying the identity of an individual user, machine, software component, or any other entity.

Availability - Whether or how often a system is available for use by its intended users. Computer, technology, and system downtime is usually costly — availability is an integral component of security and the CIA Triad (see "CIA").

B

Baseline configuration - A set of specifications or configuration items (CI) within a system that have been formally reviewed and agreed upon at a given point in time. Baseline configurations are changed through change control procedures in many of today's enterprise environments. The baseline is used as a basis for future builds, releases, or changes within a given enterprise.

Benchmark - A standard or point of reference against which things may be compared or assessed.

Black holing - A method typically used by ISPs to stop a DDoS attack on one of its customers. Black holing blocks DDoS attacks made to a given target site and renders it inaccessible to all traffic — both malicious attack traffic and legitimate user traffic.

Border router - A routing device located at an organization's boundary to an external network.

Buffer overflow - A condition within a software interface under which more input is placed into a buffer

exceeding buffer capacity — overwriting other information. Attackers exploit such a condition in order to breach, crash, or insert specially-crafted code into a system — gaining control of targeted system resources.

Business continuity - The ability to maintain operations and services — both technology and business — in the event of a disruption to normal operations and services. Business continuity ensures that any impact or disruption of services is within a documented and acceptable recovery time period. The system or operations is/are resumed at a documented and acceptable point in the processing and recovery cycle.

Business resilience - The capacity to maintain functions and organizational structure in the event of an internal or external change or threat. Business resilience recovers from a significant disruption and continues critical operations with minimal impact.

C

Capacity planning - The process used to determine whether a service, application, or process is sufficient to handle volumes at peak times and meet growth projections. Planning analysis considers hardware (e.g., networks, servers, routers, etc.), software, and personnel.

Change management - The broad processes for managing organizational change. Change management is comprised of planning, oversight or governance, project management, testing, and implementation.

CHIPS - A private-sector U.S. dollar funds transfer system, clearing and settling cross-border and domestic payments.

CIA - Confidentiality, Integrity, and Availability is commonly referred to as the "CIA Triad." CIA is at the heart of information security (InfoSec). It is the protection of information, intellectual property, privacy, and technology from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction.

Certification - Assures that a system meets defined requirements and is aligned to specified security controls. (Certification is the exercise used to support the accreditation decision process.)

Classification - Categorization (i.e., confidential, sensitive, or public) of the information processed by the service provider on behalf of the receiver organization.

Cloud computing - Generally a migration from owned resources to shared resources on the Internet. Client users receive information technology services on demand from third party service providers via the Internet "cloud." (Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data versus local server or personal computer use.)

Common Control Provider – The CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls. (CCPs are information assurance controls inherited by information systems.)

Compliance assurance - Compliance means conforming to a rule, such as a specification, policy, standard or law. The assurance or management of the same is to look after all the plus and minus of something. Regulatory compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations. Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance

controls. In many cases compliance frameworks (such as COBIT) or standards (NIST) inform on how to comply with regulations by building and supporting an effective compliance assurance framework. Also, there are a number of other regulations which apply in different fields, such as PCI-DSS, GLBA, FISMA, Joint Commission, and HIPAA.

Computer security - Security tools and managerial procedures applied to computer or technology systems to ensure the availability, integrity, and confidentiality of information managed by the systems.

Confidentiality - Assuring information will be kept secret with access limited to appropriate individuals — an integral component of security and the CIA Triad (see "CIA").

Configuration management - The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, testing, test fixtures, and test documentation. Configuration management is performed throughout the development and operational life and lifecycle of an enterprise.

Contingency plan - A plan for emergency response, backup operations, and post-disaster recovery — maintained by an organization as a component of its security program.

Contingency planning - Effective contingency planning ensures the availability of critical resources and facilitates for the continuity of operations in an emergency situation. Contingency planning is comprised of controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

Control requirements - Process used to document and/or track internal processes to determine that established procedures and/or physical security policies are being effectively followed.

Control self-assessment - A technique used to internally assess the effectiveness of risk management and control processes.

Conversion plan - A plan detailing implementation issues and transition planning in the period between the execution of an outsourcing agreement and the full production use of the outsourced services.

Corrective control - A mitigating technique designed to lessen the impact to the institution when adverse events occur.

Crisis management - The process of managing an organization and its operations in response to an emergency or event that threatens business continuity. (An organization's ability to communicate with employees, associates, customers, and the media, using technology and intervention methods is a key component of effective crisis management.)

Critical system (infrastructure) - The technology systems and organizational assets that comprise a physical or virtual environment. They are identified as critical to the operational efficacy and are critical path to the organization's tactical and strategic operations.

Custom redirect service - This service enables control over the location of incoming calls or the redirection of calls to various locations or pre-established phone numbers to ensure customer service continuity.

Cyber attack - An attempt to damage, disrupt, or gain unauthorized access to a computer, system, or electronic communications network. (An attack launched through cyberspace, targeting an organization

for purposes of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure.)

Cyber event - A cybersecurity change or occurrence that impacts operations including an organization's mission, capabilities, or reputation.

Cyber incident - Actions taken through the use of computer networks that result in an actual or potentially adverse effect on a system or its data.

Cyber resilience - The ability of a system or domain to withstand cyber attacks, failures, threats, and in such events — to reestablish itself quickly.

Cyber threat - An internal or external event, action, occurrence, or person with the potential to exploit technology-based vulnerabilities. An exploit may also adversely impact operations, organizational assets including data and systems, individuals, other organizations, and society.

Cybersecurity - The process of protecting data, consumer, financial, bank, intellectual property, and privacy information by preventing, detecting, and responding to attacks.

Cybersecurity resilience framework - A set of industry standards and best practices to help organizations manage cyber security risks.

D

DASD - Direct Access Storage Device. A magnetic disk storage device historically used in mainframe environments. DASD may also include hard drives used in personal computers.

Data center - An organization's facility used to house computer systems and components including telecommunications and storage systems.

Data classification program - Classifying data is the process of categorizing information assets based on value according to sensitivity.

Data conversion plan - Comprised of strategies involved in converting data from an existing system to another hardware platform and/or software environment.

Data corruption - Errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data.

Data integrity - The property that data has not been destroyed or corrupted in an unauthorized manner — maintaining and assuring the accuracy and consistency of data over its entire lifecycle.

Data management - The development and execution of architectures, policies, practices and procedures in order to affect managing the information lifecycle needs of an enterprise.

Data mining - The process or techniques used to analyze large sets of existing information to discover previously unrevealed patterns or correlations.

Data mirroring - A process that involves writing same data to two physical disks or servers simultaneously.

Data replication - The process of copying data usually with an objective of maintaining identical sets of

data in separate locations. Two common data replication processes used for information systems are synchronous and asynchronous mirroring.

Data synchronization - The comparison and reconciliation of interdependent data files at the same time so that they contain the same information.

Database - A collection of data that is stored on any type of computer storage medium and may be used for more than one purpose.

Daylight overdraft - A daylight overdraft occurs at any point in the business day when the balance in an organization's account becomes negative. Daylight overdrafts can occur in accounts at Federal Reserve Banks as well as at private financial institutions. Daylight credit may also emerge in the form of net debit positions of participants in private payment systems. A daylight overdraft occurs at a Federal Reserve Bank when there are insufficient funds in an organization's Federal Reserve Bank account to cover outgoing funds transfers or incoming book-entry securities transfers. An overdraft may also be the result of other payment activity processed by the Federal Reserve Bank, such as check or automated clearinghouse transactions.

DDoS - Distributed Denial of Service. A type of attack that makes a computer or system resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary — it generally consists of the concerted efforts of a group that intends to affect an organization's reputation by preventing an Internet site, service, or application from functioning efficiently. (A Denial of Service attack is different from a DDoS attack. The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and Internet connections to flood a targeted resource or system.)

Debit card - A payment card issued as either a PIN-based debit (ATM) card or as a signature-based debit card from one of the bankcard associations. A payment card issued to a person for purchasing goods and services through an electronic transfer of funds from a demand deposit account rather than using cash, checks, or drafts at the point-of-sale.

Debit entry - An entry to the record of an account to represent the transfer or removal of funds from the account.

Dedicated Synchronous Optical Network (a.k.a. SONET) - SONET is a standard for telecommunications transmissions over fiber optic (or fibre optic) cables. SONET is self-healing if a break occurs in one of its lines. When a break occurs, it uses a backup redundant ring to ensure transmission continues without interruption. SONET networks transmit voice and data over optical networks.

Deep packet inspection - The capability to analyze network traffic to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations.

Defense-in-depth - Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Deferred net settlement - See "NSS - National Settlement Service".

Deliverable - A project goal, agile sprint, or expectation. Deliverables include broadly-defined, project, sprint, or phase requirements and specifically-defined tasks within a given project or sprint.

Depository - **An institution that holds funds or marketable securities for safekeeping. Depositories may be privately or publicly operated and allow securities transfers through book-entry and offer fund accounts permitting fund transfers as a means of payment.**

Depositary bank - **The institution at which a check is first deposited. (While this term is often used interchangeably with "depository," the definition of "depositary" is a term of art in laws and regulations related to check processing.)**

Depository bank (Check 21) - **Also known as Bank of First Deposit (BOFD). The first bank to which a check is transferred even though it is also the paying bank or the payee. A check deposited in an account is deemed to be transferred to the financial institution holding the account into which the check is deposited — even though the check is physically received and endorsed first by another financial institution. Also, the Check 21 Act lets banks take advantage of image technologies and electronic transport while not being dependent on other banks being ready to settle transactions with images instead of paper.**

Detective control - **A mitigating technique designed to recognize an event and alert management when this type of event occurs.**

Dictionary attack - **Attack techniques used for defeating a cipher or authentication mechanism associated with a target computer system by trying to determine and defeat its decryption key or passphrase. For example, an attacker may attempt hundreds or sometimes millions of candidate possibilities against a computer's password authentication process by using words in a dictionary.**

Digital certificate - **The electronic equivalent of an ID card that authenticates the originator of a digital signature.**

Direct data feed - **A process used by information aggregators to gather information directly from a website operator rather than copying it from a displayed webpage.**

Direct debit - **Electronic transfer, usually through ACH, out of an individual's checking (or savings) account to pay bills, such as mortgage payments, insurance premiums, and utility payments. Also, direct debit may be referred to as "direct payment."**

Direct deposit - **Electronic deposit or credit of money by a payer directly into a payee's deposit or bank account. ACH and other deposit service providers are used to direct deposit payments, such as Social Security benefits, income from investments, CDs, annuities, and mutual funds.**

Direct presentment - **Depositary banks may present checks directly to the paying institution. The paying institution may be the depositary bank (no settlement is needed). However, when the paying institution is not a depositary bank, then the check may settle on the books of the Federal Reserve using the Federal Reserve "National Settlement Service."**

Disaster recovery - **The process of recovering from major processing interruptions.**

Disaster recovery exercise - **A test of an organization's Disaster Recovery or Business Continuity Plan (BCP).**

Disaster recovery plan - **A plan that describes the process to recover from major processing interruptions.**

Disk shadowing - A backup process that involves writing images to two physical disks or servers simultaneously.

Distributed environment - A computer system with data and program resources and components physically distributed across more than one computer, such as accessing remote databases in a geographically distributed environment.

Diversity - A description of financial services sectors in which primary and backup telecommunication capabilities do not share a single point of failure.

DLP - Data Loss Prevention. A comprehensive loss prevention planning approach covers people, processes, information, and systems. A successful DLP implements policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or transitioned.

DMZ - Abbreviation for "demilitarized zone." A computer, small subnetwork, or subnet that sits between a trusted internal network (e.g., a corporate private LAN) and an untrusted external network, such as the public Internet.

DNSSEC - Domain Name System Security extensions. A technology that was developed to, among other things, protect against the threat of domain attacks by digitally "signing" data for information assurance, integrity, and data validity.

DNS server - Domain Name System server. A computer that determines Internet Protocol (IP) numeric addresses from domain names presented in a convenient, yet readable form.

DSL - Digital Subscriber Line. A technology that uses existing copper telephone lines and advanced modulation schemes to provide high-speed telecommunications to businesses and homes.

Dual control - Dividing the responsibility of a task into separate, yet accountable actions — ensuring the integrity of the process.

Due care - The responsibility that managers and their organizations have a duty to provide for information assurance to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system and/or security framework being managed.

Due diligence - Technical, functional, and financial review to verify a third party service provider's ability to deliver the requirements specified in its proposal. The intent is to verify that the service provider has a well developed plan, adequate resources, and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

E

eBanking - Electronic Banking (a.k.a. E-Banking). The remote delivery of new and traditional banking products and services through electronic delivery channels.

EBPP - Electronic Bill Presentment and Payment. An electronic alternative to traditional bill payment — allowing a merchant or utility to present its customers with an electronic bill and the payer to pay the bill electronically. EBPP systems usually fall within two models: direct and consolidation-aggregation. In the direct model, the merchant or utility generates an electronic version of consumer billing information and notifies the consumer of a pending bill — generally via email. The consumer may initiate payment of the electronically presented bill using a variety of payment

mechanisms, such as a credit card. In the consolidation-aggregation model — consumer bills are consolidated by a consolidator acting on behalf of merchants and utilities (or aggregated on behalf of the consumer) combining data from multiple bills and presenting a single source for the consumer to initiate payment. Some consolidators present bills at their own website — most support the aggregation of bills by consumer service providers such as Internet portals, financial institutions, and brokerage websites.

EBT - Electronic Benefit Transfer. A type of EFT system involving the transfer of public entitlement payments, such as welfare or food stamps, through direct deposit or point-of-sale technology (see "POS"). The recipient can be given an identification card, similar to a benefit card, and a PIN allowing access to the benefits through an electronic network.

eCommerce - Electronic Commerce (a.k.a. E-Commerce). A broad term encompassing the remote procurement and payment by businesses or consumers of goods and services through electronic systems, such as the Internet.

EDC - Electronic Data Capture. Process used for capturing and transferring encoded information on a magnetic strip from a bankcard or debit card at the point-of-sale to a processor database.

ECP - Electronic Check Presentment. Check truncation methodology in which the paper check MICR line information is captured and stored electronically for presentment. The physical checks may or may not be presented after the electronic files are delivered — depending upon the type of ECP service used.

EFAA - Expedited Funds Availability Act. See "Regulation CC".

EFT - Electronic Funds Transfer. A generic term describing any transfer of funds between parties or depository institutions through electronic data systems.

EFTA - Electronic Funds Transfer Act. The Electronic Funds Transfer Act and Regulation E are designed to ensure adequate disclosure of basic terms, costs, and rights relating to electronic funds transfer (EFT) services provided to consumers. Financial organizations or institutions offering EFT services must disclose to consumers certain information. The disclosure includes initial and updated EFT terms, transaction information, periodic statements of activity, consumer liability (potential) for unauthorized transfers, and error resolution rights and procedures. EFT services include automated teller machines, telephone bill payments, point-of-sale transfers in retail stores, fund transfers initiated through the Internet, and preauthorized transfers to or from a consumer account.

Electronic check conversion - The process by which a check is used as a source of information for the check number, customer account number, and the number that identifies the financial institution. The information is used to make a one-time electronic payment from a customer account — an electronic funds transfer. The check itself is not the method of payment.

Electronic vaulting - A backup procedure that copies changed files and transmits them to an offsite location using a batch process.

Electronically-created payment orders - Payment orders received by merchants from consumers, typically by telephone or the Internet. Payment orders are processed through a check processing system, yet are not initiated as paper checks. Also, payment orders are not subject to check law and are not warranted by the Federal Reserve Banks.

Email server - A computer that manages email traffic.

Emergency plan - **The steps to be followed during and immediately after an emergency, such as a fire, tornado, bomb threat, etc.**

Encryption - **A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that data appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.**

End user - **An individual who will utilize a product or program.**

End-of-life - **All software products have life cycles. End-of-life refers to the date when a software development company no longer provides automatic fixes, updates, or online technical assistance for the product.**

Endpoint security - **Security controls that validate the security compliance of the client system that is attempting to use the Secure Sockets Layer (SSL) and Virtual Private Network (VPN). Endpoint security controls also include security protection mechanisms, such as web browser cache cleaners. (A cache cleaner is used to remove sensitive information from a client system.)**

End-to-end process flow - **Document that details the flow of processes, considering automated and manual control points, hardware, databases, network protocols, and real-time versus periodic processing characteristics.**

End-to-end recoverability - **The ability of an organization to recover a business process from initiation (e.g., a customer contact) through process finalization, such as transaction closure.**

Enterprise architecture - **The overall design and high level plan that describes an organization's operational framework and includes its mission, stakeholders, business and customers, work flow and processes, data processing, access, security, and availability.**

Enterprise network - **The configuration of computer systems within an organization. Includes local area networks (LANs), wide area networks (WANs), bridges, applications, etc.**

Enterprise-wide - **Across an entire organization — rather than a single business department or function.**

Exploit - **A technique or code that uses a vulnerability to provide system access to an attacker. An exploit is an intentional attack to impact a target computer operating system, system utility, technology, or application program. For example, a hacker may use a software tool designed to take advantage of a flaw in a computer system for malicious purposes, such as installing malware.**

Exposure - **The potential loss to an area due to the occurrence of an adverse event.**

Exposure limit - **In reference to the settlement of operating services — this is the maximum amount an ACH originator is allowed to originate. Exposure limit amount may be based on the originator's credit rating plus historical or predicted funding requirements and type of obligation.**

External connection - **An information system or component of an information system that is outside of the authorization boundary established by the organization. In addition, the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.**

F

Federal Reserve Banks - The Federal Reserve Banks provide a variety of financial services including retail and wholesale payments. The Federal Reserve Bank operates a nationwide system for clearing and settling checks drawn on depository institutions located in all regions of the United States.

FEDI - Financial Electronic Data Interchange (a.k.a. Financial EDI). An instrument for settling invoices by initiating payments, processing remittance data, and automating reconciliation through the exchange of electronic messages.

Fedwire® - The Federal Reserve Bank's nationwide real time gross settlement electronic funds and securities transfer network Fedwire® is a credit transfer system. Each funds transfer is settled individually against an organization's reserve or clearing account on the books of the Federal Reserve. The transaction is considered an irrevocable payment as it is processed.

Fedwire® Funds Service - The Federal Reserve Banks' high-speed electronic funds transfer system. As a real-time gross settlement system, the Fedwire® Funds Service processes and settles individual payments between participants immediately in central bank money. Once processed, these payments are final.

Fedwire® Securities Service - The Federal Reserve Banks' high-speed electronic payments system for maintaining securities accounts and for effecting securities transfers. The Fedwire® Securities Service provides a real-time, delivery-versus-payment (DVP), gross settlement system that allows for the immediate, simultaneous transfer of securities against payment. Once processed, securities transfers are final.

FEMA - FEMA is an acronym for Federal Emergency Management Agency.

Fibre Channel (or Fiber Channel) - A high performance serial link supporting its own and other higher-level protocols, such as the small computer system interface, high performance parallel interface, framing protocol, and intelligent peripheral interface. The Fibre Channel standard addresses the need for very fast transfers of large amounts of information. The fast (commonly running at 2-, 4-, 8- and 16-gigabit per second rates) technology may be converted for LAN technology by adding a switch specified in the Fibre Channel standard that handles multipoint addressing. Fibre Channel gives users one port that supports both channel and network interfaces — unburdening the computers from large number of input and output (I/O) ports. Fibre Channel provides control and complete error checking over the link.

FIN - Financial application. The SWIFT FIN application within which all SWIFT user-to-user messages are input and output. (SWIFT is a global provider of secure financial messaging.)

Finality - Irrevocable and unconditional transfer of payment during settlement.

Financial authority - A supervisory institution that is responsible for safeguarding and maintaining consumer confidence in the financial system.

Financial industry participants - Financial institutions and other organizations that are involved in the banking, securities, and/or insurance industry and are regulated by supervisory authorities.

Firewall - A network security system, which monitors the incoming and outgoing network traffic based upon predetermined security rules.

FISMA – Federal Information Security Management Act. Passed as Title III of the E-Government Act (Public Law 107-347) in December 2002. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Float - Funds held by an institution during the check clearing process before being made available to a depositor. Interest may be earned on these funds.

Flowcharts - Traditional flowcharts involve the use of geometric symbols, such as diamonds, ovals, and rectangles to represent the sequencing of program logic. (Software packages are available for use to automatically create flowcharts instead of a person tasked with hand-drawing charts.)

Frame relay - A standardized high-performance WAN protocol that operates at the physical and data link layers of the Open Systems Interconnect (OSI) reference model. Frame relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. Frame relay uses existing T-1 and T-3 lines and provides high-speed connection speeds. In the United States, frame relay supports data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds.

Framing - A frame is an area of a webpage that scrolls independently of the rest of the webpage. Framing generally refers to the use of a standard frame containing information, such as company name and navigation bars. (In this example of a webpage presentation — the frame remains on the screen while the user moves around the text in another frame or webpage section.)

FS-ISAC - Financial Services Information Sharing and Analysis Center. A nonprofit information-sharing forum established by financial service industry participants to facilitate public and private sector sharing of physical and cybersecurity threat and vulnerability information.

FTP - File Transfer Protocol. A standard high-level protocol for transferring files from one computer to another and may be implemented as an application or utility level program.

Full duplex - A communications channel that carries data in both directions.

Full-interruption/full-scale test (IT and Staff) - A business continuity test that activates all the components of the disaster recovery plan at the same time. Hardware, software, staff, communications, utilities, and alternate site processing may be thoroughly tested in this type of testing activity. The exercise may include business line end users and IT groups to ensure that each business line tests its key applications and is prepared to recover and resume its business operations in the event of an emergency. The full test verifies that systems and staff can recover and resume business within established recovery time objectives. End users may verify the integrity of the data at the alternate site after the IT groups have restored systems and applications needed for the staff to perform production activities.

Functional drill/parallel test - This test involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the Business Continuity Plan (BCP).

Functional requirements - The business, operational, and security components of a business project. They define the goals and scope of work that a project team needs while providing objective ways to measure team success.

Functionality testing - A test designed to validate that a business process or activity accomplishes expected results.

G

Gap analysis - A comparison that identifies the difference between actual and desired outcomes.

Gateway server - Used to enable agent-management of computers that are outside the trust boundary of management groups, such as in a domain.

General controls - Other than application controls, these are those controls that relate to the environment. It's in this environment that application systems are developed, maintained, and operated, and that are applicable to all the applications in an organization. (The objectives of general controls are to ensure acceptable development, implementation of systems, integrity of program and data files plus computer operations. Like application controls — general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IT strategy and an IT security policy. Also, the IT staff is organized to separate conflicting duties when planning for disaster prevention and recovery.)

GETS - Acronym for the Government Emergency Telecommunications Service card program. GETS cards provide emergency access and priority processing for voice communication services in emergency situations.

GLBA - Gramm-Leach-Bliley Act. The GLBA, also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999). It requires Federal banking agencies to establish information security standards for financial institutions.

Governance - In computer security, governance is the setting of clear expectations for the conduct (i.e., behaviors and actions) of the entity being governed. Governance directs, controls, and strongly influences an entity to achieve an organization's expectations. Governance includes specifying a framework for decision making with assigned decision rights and accountability — intended to consistently produce desired behaviors and actions.

Grandfather-father-son - Refers to a common rotation scheme for backup media and is comprised of three or more backup cycles, such as daily, weekly, and monthly. Daily backups are rotated on a daily basis using a first in, first out system. Weekly backups are rotated on a weekly basis and the monthly backup is rotated on a monthly schedule. Also, quarterly, half-yearly, and annual backups may be separately retained and rotated. (In addition, BCP and safekeeping policies may dictate that some backups are removed from an IT service area and moved to an offsite facility for safekeeping and/or disaster recovery.)

H

Hacker - A hacker is an individual or a group who seek to exploit weaknesses in a target computer system or network.

Haircut - With respect of an eligible currency, the percentage increase of a negative currency balance or reduction of a positive currency balance and is based on (a) the volatility of the historic foreign exchange movements in the applicable eligible currency determined by CLS Bank (i.e., originally Continuous Linked Settlement) and (b) an add-on component.

Hardening - The process of securing a computer’s administrative functions or inactivating those

features not needed for the computer's intended business purpose.

Hardware - The physical elements of a computer system — the computer equipment as opposed to programs or information stored in a machine.

Hash - A fixed length cryptographic output of variables, such as a message being operated on by a formula or cryptographic algorithm.

Hash totals - A numerical summation of one or more corresponding fields of a file that would not ordinarily be summed. In addition, hash totals may be used to detect when changes in electronic information have occurred.

HBA - Host Bus Adapter. A host bus adapter provides I/O processing and physical connectivity between a server and storage. As the only part of a storage area network that resides in a server — HBAs also provide a critical link between the storage area network and the operating system and application software.

HHS – The United States Department of Health and Human Services. HHS protects the health of all Americans and provides essential human services, especially for those who are least able to help themselves.

Hijacking - The use of an authenticated user's communication session to communicate with system components.

Hop - Each step of a trip a data packet takes from its origination to its destination. For example, on the Internet — a data packet may go through several routers (i.e., each router is counted as a hop) before reaching its final destination.

Host - A computer that is accessed by a user from a remote location.

Hosting - See "Website hosting".

HSM - Hierarchical Storage Management. HSM is used to dynamically manage the backup and retrieval of files based on how often they are accessed using storage media and devices that vary in speed and cost.

HTML - Abbreviation for "Hypertext Markup Language." A set of codes that can be inserted into text files to indicate special typefaces, inserted images, and links to other hypertext documents.

Hub - Simple devices (e.g., Ethernet Hub) that pass all data traffic in both directions between the LAN sections they link. Hubs forward every message they receive to the other sections of the LAN. (Hub forwarding includes data traffic that may not need to be forwarded to those other sections.)

HVAC - Heating, Ventilation, and Air Conditioning.

Hyperlink - A linked item on a webpage which when selected transfers user control directly to another location in a hypertext document, webpage, or website.

Hypervisor - A piece of software that provides abstraction of all physical resources, such as central processing units, memory, network, and storage. It enables multiple computing stacks (i.e., consisting of

an operating system, middleware and application programs) called virtual machines to be run on a single physical host.

I

I/O - Input/output.

IDS - Intrusion Detection System. A device or software application that monitors network, system activities, and/or policy violations and produces electronic reports. A host-based IDS uses system log files and other electronic audit data to identify suspicious activity. A network-based IDS uses a sensor to monitor packets on the network to which it is attached.

Image archive (Check 21) - Database for storage and easy retrieval of check images.

Image capture (Check 21) - The process of digitizing both sides of physical items and their assorted MICR information as they are processed at the Federal Reserve Bank. Also, includes storage of the images for up to 60 days.

Image exchange (Check 21) - Exchange of some or all of the digitized images of a check.

Implementation plan - A plan that details project management requirements and issues to be addressed during a period between execution of an outsourcing agreement and full production use of outsourced services.

Incident management - The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit incident disruption and restore operations as quickly as possible.

Incident response plan - A plan that defines incident response action steps, involved resources, and communication strategy upon identification of a threat or potential threat event. For example, threat events as in a breach in security protocol, power, telecommunication outages, severe weather, or workplace violence.

Indemnifying bank (Check 21) - A financial institution that transfers, presents, returns a substitute check, paper, or electronic representation of a substitute check for which it receives consideration. (The financial institution shall indemnify the recipient and any subsequent recipient including a collecting or returning financial institution, depository financial institution, drawer, drawee, payee, depositor, and any endorser for any loss incurred by any recipient of a substitute check if that loss occurred due to the receipt of a substitute check instead of the original.)

Independence - Self-governance is the freedom from conflict of interest and undue influence. The IT auditor is free to make her own decisions — not influenced by the organization being audited or by its managers, employees, and associates.

Industry testing - A test designed to validate business processes integrated across firms within the financial industry. Test cases support business continuity objectives of an individual organization or a collective representation of firms.

Information Owner/Steward – An official in an organization with statutory, operational, and management authority for specified information. The Steward has oversight and responsibility for establishing policies and procedures governing its creation, collection, processing, dissemination, and disposal.

Information security - **The process by which an organization protects the creation, collection, storage, use, transmission, and disposal of information.**

Information System Owner – **The ISO is an official of an organization responsible for procurement, development, modification, integration, operation, maintenance, and disposal of an information system.**

Information systems - **Electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems may include networks (computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems). Other examples are backup tapes, mobile devices, and other media.**

Information technology - **Any computer services, equipment, interconnected systems, or subsystems of equipment that comprise an organization's IT architecture or infrastructure. It may include computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources.**

Infrastructure - **Describes what has been implemented by IT architecture. May include support facilities such as power, cooling, ventilation, server, data redundancy and resilience plus telecommunication lines. Specific architecture types may exist for the following — enterprise, data, technology, security, and application.**

Instruction - **Means (i) any instruction submitted by a member through the submission process directing CLS Bank to settle certain payment entitlements and obligations arising pursuant to an FX transaction eligible for settlement in CLS Bank and (ii) any instructions resulting from the split of Settlement Eligible Instructions.**

Integrated test/exercise - **This integrated test/exercise incorporates more than one component or module, as well as external dependencies to test the effectiveness of the continuity plans for a business line or major function.**

Integrity - **Assurance that information is trustworthy and accurate. It ensures that data is not accidentally or maliciously altered or destroyed — it's an integral component of security and the CIA Triad (see "CIA" and "Data integrity").**

Interbank checks - **Checks that are not "on-us." They are cleared and settled either by direct presentment, a clearinghouse association, a correspondent bank, or a Federal Reserve Bank.**

Interchange - **Exchange of transactions between financial institutions participating in a bank card network — based on a common set of rules. Card interchange allows a financial institution's customer(s) to use a bank credit card at any card honoring merchant and to gain access to multiple ATM (Automated Teller Machine) systems from a single ATM.**

Interchange (fees) - **Fees paid by one financial institution to another to cover handling costs and credit risk in a financial institution card transaction. Interchange fees generally flow toward the institution funding the transaction and assuming the risk. In a credit card transaction, the interchange fee is paid by the merchant acquirer accepting the merchant's sales draft to the card-issuing institution, which passes the fee to its merchants. In EFT/POS transactions, interchange flows in the opposite direction —**

the card-issuing institution (or customer) pays the fee to the terminal-owning institution. When a transaction is an off-line debit sale, the card-issuing institution collects an interchange fee from the merchant, rather than from the customer unlike in an EFT/POS transaction where the customer pays the interchange fee. Interchange revenue is derived from fees set by the card associations. Depending on the card association — fees may range from 1% to 3% of the value of the transaction. (Interchange revenue is recognized as a card issuer's second largest revenue line item.)

Interconnectivity - The state or quality of being connected together. The interaction of a financial institution's internal and external systems and applications and the entities with which they are linked.

Interdependencies - Where two or more departments, processes, functions, and/or third-party providers support one another.

Interface - Computer programs that translate information from one system or application into a format required for use by another system or application.

Internet - A public facing worldwide network of computers and networks governed by standards and protocols developed by the Internet Engineering Task Force (IETF).

Intranet - An organization's internal facing private network accessible only by its staff. (The Intranet IT systems of an organization provide a wide range of information and services that are not available to the public from the Internet.)

Interoperability - The ability of a system to work with or use the parts or equipment of another system.

Interoperability standards/protocols - Commonly agreed upon standards that enable different programs to share information. For example, HTTP (Hypertext Transfer Protocol) is a standard method of publishing information as hypertext in HTML format on the Internet.

Intrusion detection - Techniques that attempt to detect unauthorized entry or access into a system, computer or network by observation of threat actions, security log review, and audit data assessment. (Early detection is key to effectively identifying system security break-ins.)

IP - Internet Protocol. IP is a standard format for routing data packets between computers. IP is efficient, flexible, routable, and widely used with many applications, and is gaining acceptance as a preferred communication protocol suite.

IPS - Intrusion Prevention System. A network security/threat prevention system that detects and stops threat activity when identified as an intrusion — ideally before it reaches its target.

IPv6 - Version 6 of the Internet Protocol.

ISAC - Information Sharing and Analysis Center.

ISACA® - Previously known as the Information Systems Audit and Control Association. ISACA® is a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance.

iSCSI - Internet Small Computer System Interface. An Internet protocol-based storage networking standard for linking data storage facilities. It's used to facilitate data transfers over intranets and manage storage over long distances. iSCSI works on top of the Transport Control Protocol (TCP) and

allows the SCSI command to be sent end-to-end over local-area networks (LANs), wide-area networks (WANs), or the Internet.

ISDN - Integrated Systems Digital Networking. A telecommunication network through which sound, images, and data can be transmitted as digitized signals. (A hierarchy of digital switching and transmission systems that provides voice, data, and image in a unified manner. ISDN is synchronized in that all digital elements communicate in the same protocol at the same speed.)

ISO - International Organization for Standards.

ISP - Internet Service Provider. A company that provides its customers with access to the Internet (e.g., AT&T, Verizon, CenturyLink).

IT architecture - A subset of enterprise architecture with detail to support data processing and access. IT architecture includes fundamental requirements for centralized or distributed computing, real or virtual servers, devices and workstations, and networking design. Plans may also exist for data, security, and applications within the domain of IT architecture.

Iterative - Repetitive or cyclical. Iterative software development involves the completion of project tasks or phases in repetitive cycles. Tasks and phase activities are repeated until a desired result is achieved.

IT governance - An integral part of governance that consists of an organization's leadership, organizational structures, and processes to ensure that IT sustains and extends its strategies and objectives.

IT strategic plan - A comprehensive blueprint that guides the organization's technology management. It contains high-level goals and plans for all areas of information technology that affect the business — not just the infrastructure.

IT system inventory - A list containing information about the system resources owned or operated by an organization.

K

Key fob - A small portable device equipped with chip technology allowing the holder the ability to access network systems, such as those used for payments and to store personal data. In addition, a key fob is identified as type of security token with built-in authentication mechanisms. Fobs are also used with car and motorcycle starters, garage door openers, and keyless entry devices on hotel room doors.

Kiosk - A publicly accessible computer terminal or technology medium that permits customers to directly communicate with a financial institution, pubic service pension, and other organizational services via a network.

L

LAN - Local Area Network.

LAR - Legal Amount Recognition. The handwritten dollar amount of the check.

Large value funds transfer system - A wholesale payment system used primarily by financial institutions in which large values of funds are transferred between parties. Fedwire® and CHIPS are used as large-value transfer systems in the United States.

Legacy systems - **A term commonly used to refer to existing, yet dated computer systems and applications with which new systems or applications may exchange information with for a limited time.**

Life cycle process - **A multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.**

Lockbox - **Deposit mechanism used by commercial firms and businesses to facilitate their deposit transaction volume. (Typically, commercial firms and businesses direct customers to send payments directly to a financial institution address or post office box controlled by the institution. Financial institution personnel record payments received and prepare deposit slips — subsequent processing proceeds as with other deposit taking activities.)**

Lockout - **The action of temporarily revoking network or application access privileges due to repeated unsuccessful logon attempts.**

Long position - **In respect of a currency balance that is greater than zero — the amount by which such currency balance is greater than zero. A position that appreciates in value if market prices increase. For example, when one buys a currency — their position is long.**

M

Mainframe - **An industry term for a large computer. A mainframe computer may be used for commercial applications of businesses and other large-scale computing purposes. A mainframe is associated with centralized rather than distributed computing.**

Malware - **Software designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of covert, hostile, intrusive, threatening or annoying software, script or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software, script or programs.**

Management controls – **Security controls that are strategic and suitable for planning and monitoring purposes. (Selecting proper controls and implementing those will initially help an organization or agency to bring down risk to acceptable levels.)**

Man-in-the-middle attack - **Places an attacker's computer in the communication line between the server and the client. The attacker's machine may monitor and change communication or data.**

Market-wide tests - **Market-wide tests are also called cross-market tests or "street tests" that are sponsored by the Securities Industry Association, Bond Market Association, and Futures Industry Association. These tests validate the connectivity from alternate sites and include transaction, settlement, and payment processes — to the extent practical.**

Matched instructions - **Two Instructions in which the information set forth in a specific CLS Bank Rule is matched in accordance with parameters and procedures set forth in the CLS Bank Rules.**

Matching - **With respect to compared and non-compared transactions — the process of comparing the trade or settlement details provided by counterparties to ensure they agree with respect to the terms of the transaction. Also, matching is called comparison checking.**

Media - **Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).**

Merchant acquirer - Bankcard association members who initiate and maintain contractual agreements with merchants for the purposes of accepting and processing bankcard transactions.

Merchant processing - Activity for the acceptance and settlement of bankcard products and transactions from merchants through a payment system.

Metric - A quantitative measurement.

MICR - Magnetic Ink Character Recognition. Magnetic codes found on the bottom of checks, deposit slips, and general ledger debit and credit tickets that allow a machine to scan (capture) the information. MICR encoding on a check includes the account number, routing number, serial number of the check, and the amount of the check. (The amount of the check is encoded when the proof department processes the check.)

Microwave technology - A narrowband technology, which requires a direct line-of-sight communication medium to transmit voice and data communications. It is used to integrate a broad range of fixed and mobile communication networks.

Midrange - Computers that are more powerful and capable than personal computers but less powerful and capable than mainframe computers.

Milestone - A major project event.

MIPS - Millions of instructions per second. A general measure of computing performance — the amount of work a larger computer may perform.

Mirroring - A process that copies data to multiple disks over a computer network in real time or close to real time.

MIS - Management Information Systems. A general term referring to computer-based systems in an enterprise providing managers with tools to organize, evaluate, and manage departments within various organizations.

Mnemonic - A symbol or expression that can help someone remember something. For example, the phrase "Hello! My name is Bill. I'm 9 years old." might help an individual remember a secure 10-character password of "H!MniBI9yo."

Mobile device - A portable computing and communications device with information storage capability. Examples include notebook and laptop computers, cellular telephones and smart phones, tablets, digital cameras, and audio recording devices.

Mobile financial services - A financial institution's use of mobile devices to provide products and services to its customers.

Modeling - The process of abstracting information from tangible processes, systems and/or components to create a paper design or computer-based representation of an enterprise-wide or business line activity.

Module - A combination of various components of a business process or supporting system.

Module test/exercise - A test designed to verify functionality of multiple components of a business line or supporting functions at the same time.

Moral Turpitude - A phrase used in Criminal Law to describe conduct that is considered contrary to community standards of justice, honesty, or good morals.

Multi-factor authentication - The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number), something you have (e.g., cryptographic identification device or token), and something you are (i.e., biometric).

Multilateral netting settlement system - Multilateral netting is an arrangement among three or more parties to net their obligations. Settlement system transfers are irrevocable, yet are only final after the completion of end-of-day-settlement.

Multiplexers - A device that encodes or multiplexes information from two or more data sources into a single channel. They are used in situations where the cost of implementing separate channels for each data source is more expensive than the cost and inconvenience of providing the multiplexing/de-multiplexing functions.

N

NACHA – The National Automated Clearing House Association. The national association establishes the rules and procedures governing the exchange of ACH payments. Participating financial institutions use the rules to transfer funds electronically.

NAS - Network Attached Storage. NAS systems usually contain one or more hard disks that are arranged into logical redundant storage containers much like traditional file servers. NAS provides readily available storage resources and helps alleviate performance bottlenecks associated with access to storage devices (see "NAS").

Net debit cap - The maximum dollar amount of uncollateralized daylight overdrafts that an institution is authorized to incur in its Federal Reserve account. The net debit cap is generally equal to an institution's capital — times the cap multiple for its cap category.

Network - Two or more computer systems that are grouped together to share information, software, and hardware resources.

Network activity baseline - A base for determining typical network utilization patterns for the purposes of identifying significant deviations.

Network administrator - The individual responsible for the installation, management, and control of a network or networks.

Network diagram - A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or arrangement of a network including its nodes and connecting communication lines.

Network security - The protection of computer networks and their services from unauthorized entry, modification, destruction, threat, or disclosure. The provision of assurance for network security is that the network performs its critical functions correctly and that there are no harmful side effects. Network security includes providing for data integrity and upholds all of confidentiality, integrity, and availability (i.e., CIA Triad).

**NIST - National Institute of Standards and Technology. An agency of the U.S. Department of Commerce that works to develop and apply technology,
measurements, and standards. NIST developed a voluntary cybersecurity framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructures.**

Non-repudiation - Ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

NSS - National Settlement Service. Also, referred to as Deferred Net Settlement. The Federal Reserve Banks' multilateral settlement service. NSS is offered to depository institutions that settle for participants in clearinghouses, financial exchanges, and other clearing and settlement groups. Settlement agents acting on behalf of those depository institutions electronically submit settlement files to the Federal Reserve Banks. Files are processed on receipt and entries are automatically posted to the depository Reserve Bank institution accounts. Entries are final when posted.

O

Object code - Software program instructions compiled (translated) from source code into machine-readable formats.

Object program - A program that has been translated into machine language and is ready to be run (i.e., executed) by the computer.

ODFI - Originating Depository Financial Institution. A participating financial institution that originates entries at the request of and by agreement with its originators in accordance with the provisions of NACHA rules.

OFAC - Office of Foreign Assets Control. The United States Department of the Treasury, Office of Foreign Assets Control, administers and enforces economic sanction programs primarily against countries and groups of individuals such as terrorists and narcotics traffickers. The sanctions may be either comprehensive or selective — using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

Offsite rotation - Used for backup and/or disaster recovery — a scheduled or on demand move of a copy of a database, information, file, or tape to an offsite storage facility to be used in an emergency or recovery need.

On-us checks - Checks that are deposited into the same institution on which they are drawn.

Open market operations - The buying and selling of government securities in the open market in order to expand or contract the amount of money in the banking system.

Operating system - A system that supports and manages software applications and computer resources. Operating systems allocate system resources, provide access and security controls, maintain file systems, and manage communications between end users and hardware devices.

Operational controls – Controls used in day-to-day operations to ensure the secure execution of business activities. For example, controls are mechanisms or tools for IT support and operations, information

security incident-handling procedures and processes, and physical and/or environmental security controls.

Operational IT plan - IT operational planning is focused on specific procedures and processes that implement or contribute to a larger strategic plan.

Operational risk - A risk of failure or loss resulting from inadequate or failed processes, people, or systems.

Organizational maturity – A reflection of how well an organization manages internal processes, changes, and responses to unexpected events. Organizational maturity is important in determining an effective information and compliance assurance program. A number of organizational maturity models exist for the industry at large, such as Capability Maturity Model (i.e., CMM or CMMI), Information Technology Infrastructure Library (ITIL), and Organizational Change Maturity Model (OCMM).

Originator - A person has authorized an ODFI to transmit a credit or debit entry to the deposit account of a receiver at an RDFI.

Outsourcing - The practice of contracting with another entity to perform services that might otherwise be conducted in-house. Contracted relationship with a third party to provide services, systems, or support.

P

P2P - Peer-to-Peer communication. The communications that travel from one user's computer to another user computer without being stored for later access on a server. Email is not a P2P communication since it travels from a sender to a server and is retrieved by a recipient from the server. However, "Online Chat" is a P2P communication tool since messages travel directly from one user to another.

P2P - Person-to-person payments. An online payment technology using electronic mail messaging to invoke a transfer of an item of value between each participating parties over existing proprietary networks as an on-us transaction.

Pandemic - An epidemic or infectious disease that may have a worldwide impact.

Passwords - A secret sequence of characters and/or symbols used as a means of authentication.

Patch - Software code replacing or updating other code. (Patches are used to correct security flaws and declining software features.)

Patching - Software code replacing or updating other code. Maintaining active patching with current patches helps to overcome security flaws, system exposure, threat vehicles, and declining software features.

Paying bank - A paying bank is the institution where a check is payable and to which it is sent for payment.

Payment - A transfer of an item of value from one party to another.

Payment system - Payment mechanisms, rules, institutions, people, markets, and agreements making an exchange of payment possible.

Payroll card account - **A bank account that is established directly or indirectly by an employer on behalf of an employee. Electronic funds are transferred to the account on behalf of the employee's wages or compensation. The payroll card, often branded by one of the credit/debit card associations, provides the employee access to transferred funds.**

PBX - **Private Branch Exchange. A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines.**

PCI Security Standards Council - **The governing body, representing key participants of the payment card industry, which establishes and maintains security standards for payment cards.**

PDA - **Personal Digital Assistant. A pocket-sized, special purpose personal computer that may lack a conventional keyboard.**

PDH - **Plesiochronous Digital Hierarchy. PDH is a technology used in telecommunications networks to transport large quantities of data over digital transport equipment, such as fiber optic (or fibre optic) and microwave radio systems.**

Penetration test - **The process of using approved, qualified personnel to conduct real-world attacks against a system to identify and correct security weaknesses and vulnerabilities before they are discovered and exploited by others.**

Phase - **A project segment within project lifecycle management.**

Phishing - **A digital form of social engineering that uses authentic-looking — but bogus — email to request personal demographic information from users or direct them to a fake website that request personally identifiable information (see "PII data").**

PII data - **Personally Identifiable Information (PII) or Sensitive Personal Information (SPI). Used in United States privacy law and information security. Its information that may be used on its own or with other information to identify, contact, locate a single person, or to identify an individual in context (see "Sensitive customer information").**

PKI - **Private Key Infrastructure. The use of public key cryptography in which each customer has a key pair (i.e., a unique electronic value called a public key and a mathematically-related private key). The private key is used to encrypt (sign) a message that can only be decrypted by the corresponding public key or to decrypt a message previously encrypted with the public key. The public key is used to decrypt a message previously encrypted (signed) using an individual's private key or to encrypt a message so that it can only be decrypted (read) using the intended recipient's private key.**

Platform - **The underlying computer system on which application programs run. Platform computing provides software that dynamically connects IT resources to workload demand, as based upon business policies and workload performance rules.**

POD - **Proof of Deposit. The verification of the dollar amount written on a negotiable instrument being deposited.**

POS - **Point-of-Sale network. A network of institutions, debit cardholders, and merchants that permit consumers to make direct payment electronically at the place of purchase. At POS time, payment funds are withdrawn from the account of the cardholder.**

Pop-up box - **A dialog box that automatically appears when a person accesses a webpage.**

Port - **Either an endpoint to a logical connection or a physical connection to a computer.**

POTS - **Plain Old Telephone System. Basic telephone service.**

Presentment fee - **A fee that an institution receiving a check may impose on the institution that presents the check for payment. No presentment fee may be charged for checks presented by 8 a.m. local time.**

Preventive control - **A mitigating technique or detective control designed to detect and prevent errors or event irregularities.**

Principle of least privilege - **The security objective of granting users only the access needed to perform official duties.**

Privacy Law: Collection Limitation Principle – **There are limits to the collection of personal data. Data is obtained by lawful and fair means with the knowledge or consent of the data subject – where appropriate.**

Privacy Law: Data Quality Principle – **Personal data is relevant to the purposes for which it is to be used. To the extent necessary for those purposes – it must be accurate, complete, and maintained.**

Privacy Law: Purpose Specification Principle – **Personal data is collected for purposes specified not later than at the time of data collection. Subsequent use is limited to the fulfillment of the stated purposes. (If the data are used after the time of data collection for a purpose not stated at the time of collection, then that use must be specified on each occasion.)**

Privacy Law: Security Safeguards Principle – **Personal data is to be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.**

Privacy Law: Use Limitation Principle – **Personal data is not to be disclosed, made available, or otherwise used for purposes other than those specified in accordance with these privacy law principles except with the consent of the data subject or by the authority of law.**

Private label card - **See "Store card".**

Privileged access - **Individuals with the ability to override system or application controls.**

Project - **Tasks involving acquisition, development, or maintenance of a technology product.**

Project management - **Planning, monitoring, and controlling tasks and activities.**

Protocol - **A format for transmitting data between devices.**

Proxy server - **An Internet server that controls a client's computer access to the Internet. Using a proxy server, a company can stop employees from accessing undesirable websites, improve performance by storing webpages locally, and hide the internal network's identity so monitoring is difficult for external users.**

PSR - Payments System Risk Policy. The Federal Reserve's Payments System Risk (PSR) policy addressing risks that payment systems present to the Federal Reserve Banks, the banking system, and to other sectors of the economy.

PVC - Permanent Virtual Circuit. PVC is a pathway through a network that is predefined and maintained by the end systems and nodes along the circuit, yet the actual pathway through the network may change due to routing issues. PVC is a fixed circuit that is defined in advance by the public network carrier. (Refer to "SVC - Switched Virtual Circuit" for additional discussion.)

Public key - See "PKI".

R

RAID - Redundant Array of Independent Disks. The use of multiple hard disks to store the same data in different places. By placing data on multiple disks, I/O operations can overlap in a balanced way — improving performance. Multiple disks in a RAID increases mean time between failure (MTBF), yet storing data redundantly also increases fault-tolerance.

RCC - Remotely Created Check. A check that is drawn on a customer account at a financial institution, yet is created by the payee and does not bear a signature in the format agreed to by the paying financial institution and customer. RCCs are also known as "demand drafts," "telechecks," "preauthorized drafts," "paper drafts," or "digital checks."

RDC - Remote Deposit Capture. A service that enables users at remote locations to scan digital images of checks and transmit captured data to a financial institution or a merchant that is a customer of a financial institution.

RDFI - Receiving Depository Financial Institution. Any financial institution qualified to receive debits or credits through its ACH operator in accordance with ACH rules.

Real-time network monitoring - Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.

Receiver - An individual, corporation, or other entity that has authorized an organization or an originator to initiate a credit or debit entry to a transaction account belonging to the receiver held at its RDFI.

Reciprocal agreement - A mutual agreement between two different companies with similar computer systems agree to provide each other with computer processing time in the event one of the systems is rendered inoperable. Processing time may be provided on a "best effort" or as "time available" basis. However, as a disaster recovery best practice — reciprocal agreements are not usually acceptable as a primary recovery option.

Reconverting bank (Check 21) - The financial institution that creates a substitute check. With respect to a substitute check that was created by a person that is not a financial institution — the reconverting bank is the first financial institution that transfers, presents, or returns that substitute check. Or, in lieu thereof, the first paper or electronic representation of that substitute check. The reconverting bank warrants that (1) the substitute check is the legal equivalent of the original check, and; (2) the original check cannot be presented again in any form. In this way, the customer pays the check only once.

Recovery service levels - Terms that define the speed, quality, and quantity of recovery capability in response to a disaster. A recovery service level may include recovery time objective, recovery point

objective, timely notification, and percentage of production service level agreements that will be delivered during recovery mode, etc.

Recovery site - An alternate location for processing information and possibly conducting business in an emergency. Usually distinguished as "hot" sites that are fully configured centers with compatible computer equipment and "cold" sites that are operational computer centers without the computer equipment.

Recovery vendors - Companies that provide recovery sites and support services for a fee.

Red team - A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise security posture. The red team objective is to improve enterprise information assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders in an operational environment.

Regulation CC - The Expedited Funds Availability Act. A regulation (12 CFR 229) promulgated by the Board of Governors of the Federal Reserve System regarding the availability of funds and the collection of checks. The regulation governs the availability of funds deposited in checking accounts and the collection and return of checks.

Regulation E - The Electronic Fund Transfer Act. A regulation (12 CFR 205) promulgated by the Board of Governors of the Federal Reserve System to ensure consumers a minimum level of protection in disputes arising from electronic fund transfers.

Regulation Z - The Truth in Lending Act. A regulation (TILA) (12 CFR 226) promulgated by the Board of Governors of the Federal Reserve System. The regulation prescribes uniform methods for computing the cost of credit, disclosing credit terms, and resolving errors on certain types of credit accounts.

Remittance cards - Payment cards that are typically used to facilitate cross-border movement of funds by individuals and for person-to-person transactions.

Remote access - The ability to obtain access to a computer or network from a remote location.

Remote capture - Process that is used to scan and transmit check images and data electronically.

Remote control software - Software that is used to obtain access to a computer or network from a remote distance.

Remote journaling - Process used to transmit journal or transaction logs in real time to a backup location.

Removable media - Portable electronic storage media, such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device — used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and other similar storage devices.

Replay attack - The interception of communications, such as an authentication communication and subsequent impersonation of the sender when retransmitting the intercepted communication.

Repudiation - The denial by one of the parties to a transaction of participation in all or part of that

transaction or the content of the communication.

Reserve account - A noninterest-earning balance account institutions maintain with the Federal Reserve Bank or with a correspondent bank to satisfy the Federal Reserve's reserve requirements. Reserve account balances play a central role in the exchange of funds between depository institutions.

Reserve requirements - The percentage of deposits that a depository institution may not lend out or invest and must hold either as vault cash or on deposit at a Federal Reserve Bank. Reserve requirements affect the potential of the banking system to create transaction deposits.

Residual risk - The amount of risk remaining after the implementation of controls.

Resilience - The ability of an institution to recover from a significant disruption and resume critical operations.

Resilience testing - Testing of an organization's business continuity and disaster recovery resumption plans.

Retail payments - Payments made in the goods and services market.

Retention requirement - Requirement established by an organization or by regulation for the length of time and/or for the amount of information that is retained.

Return (ACH) - Any ACH entry that has been returned to the ODFI by the RDFI or by the ACH operator because it cannot be processed. The reason for each return is included with the return in the form of a "return reason code." (See the NACHA "Operating Rules and Guidelines" for a complete reason code listing.)

Risk - The potential that events, expected or unanticipated, may have an adverse effect on a financial institution's earnings, capital, or reputation.

Risk analysis - The process of identifying risks, determining their probability and impact plus identifying areas needing safeguards, as risk analysis is an integral part of risk management.

Risk assessment - A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the organization, its customers and financial markets — rather than the nature of the threat.

Risk identification - The process of determining risks and existing safeguards. It generally includes inventories of systems and information necessary to operations and defines potential threats to systems and operations.

Risk management - Risks may come from various sources including uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or its life cycle), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or uncertain or unpredictable events. Risk management is the total process required to identify, control, and minimize the impact of uncertain events or disasters. (The objective of a risk management program is to reduce risk and obtain and maintain appropriate management approval at predefined stages in its life cycle.)

Risk measurement - A process to determine the likelihood of an adverse event or threat occurring and the potential impact of such an event on an organization. The result of risk measurement leads to the prioritization of potential risks based on severity and likelihood of occurrence.

Risk mitigation - The process of reducing risks through the introduction of specific controls and risk transfer. It includes the implementation of appropriate controls to reduce the potential for risk and bring the level of risk in line with an organization's risk policy.

Rlogin - Remote login. A UNIX utility that allows a user to login to a remote host on a network, as if it were directly connected and make use of various services. (Remote login is an information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security control.)

RMF – Risk Management Framework. RMF is the unified information security framework for the entire federal government that is replacing the legacy Certification and Accreditation (C&A) processes within federal government agencies and departments – the Department of Defense (DOD) and the Intelligence Community (IC).

Rogue wireless access - An unauthorized wireless node on a network.

Router - A hardware device that connects two or more networks and routes incoming data packets to the appropriate network.

Routing - The process of moving information from its source to its target destination.

Routing number - Also referred to as the ABA number. A nine-digit number (eight digits and a check digit) that identifies a specific financial institution.

RPO - Recovery Point Objective. RPO, or sometimes referred to in its plural form as "RPOs," is the amount of data at risk without severely impacting recovery of operations or the point in time in which systems and data must be recovered (i.e., the date and time of a business disruption).

RTGS - Real Time Gross Settlement. A type of payments system operating in real time rather than batch processing mode. It provides immediate finality of transactions. Gross settlement refers to the settlement of each transfer individually rather than netting. Fedwire® is an example of a real time gross settlement system.

RTO - Recovery Time Objective. RTO, or sometimes referred to in its plural form as "RTOs," is the maximum allowable downtime that can occur without severely impacting the recovery of operations. Or, the time in which systems, applications, or business functions must be recovered after an outage (i.e., the point in time that a process can no longer be inoperable).

S

SAN - Storage Area Network. SAN represents several storage systems that are interconnected to form one backup network, which allows various systems to be connected to any storage device and prevents dependence upon a single line of communication.

Sandbox - A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. Also, a sandbox is created and used by programmers to facilitate controlled coding, yet in a

standalone development environment shielded from production systems.

SAR - Suspicious Activity Report. Reports required to be filed by the Bank Secrecy Act when a financial institution identifies or suspects fraudulent activity.

SAS 70 report - An audit report of a servicing institution prepared in accordance with guidance provided in the American Institute of Certified Public Accountant's Statement of Auditing Standards Number 70.

Satellite technology - Satellite links efficiently extend the reach of typical communication systems to distant areas and provide alternative traffic routing in an emergency.

Scalability - A term that refers to how well hardware and software systems may adapt to increased resource and performance demands. For example, a scalable network system would be one that may begin with just a few nodes, yet can easily expand to thousands of nodes.

Scenario analysis - The process of analyzing possible future events by considering alternative possible outcomes.

Scorecard - A dashboard of performance measures.

Screen scraping - A process used by information aggregators to gather information from a target website. An aggregator accesses a target site by logging in as a customer or accesses it through the Internet and electronically reads and copies selected information from displayed webpages. Then, the aggregator pastes a redisplay of the information on their own website. The process is analogous to "scraping" the information off the target computer screen.

Script - A file containing active content. For example, commands or instructions to be executed by a computer.

SCSI - Small Computer Systems Interface (pronounced "scuzzy"). A standard way of interfacing a computer to disk drives, tape drives, and other devices that require high-speed data transfer. Also, a secondary SAN protocol that allows computer applications to utilize storage devices.

SDH - Synchronous Digital Hierarchy. SDH is an international standard technology for synchronous data transmission on optical media, such as fiber optic (or fibre optic) cable. (The North American equivalent of SDH is SONET. SDH defines a standard rate of transmission at 155.52 Mbps, which is referred to as STS-3 at the electrical level and STM-1 for SDH.)

SDLC - Systems Development Life Cycle. SDLC is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.

SEC - Standard Entry Class code. Three character codes in an ACH company/batch header record used to identify the payment type within an ACH batch.

Security architecture - A detailed description of all aspects of the system that relate to security along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy security requirements.

Security audit - An independent review and examination of system records. Audit activities are designed

to test for adequacy of system controls, ensure compliance with established policies and operational procedures plus recommend any indicated changes in controls, policies, and procedures.

Security breach - A security event that results in unauthorized access of data, applications, services, networks, or devices by bypassing underlying security mechanisms.

Security control and outsourcing – Once an outsourcing service is used including cloud and IT security services – the service provider's employees may have direct access to and potential control of an organization's or agency's information assets. In a business first model, priority is given to service contract and service level agreements, which are established to clearly spell out how information assurance is to be managed. (Refer to "ISO/IEC 17799," which provides a list of the items to be considered in producing a contract and SLA.)

Security event - An event that potentially compromises confidentiality, integrity, availability (i.e., CIA Triad) or accountability of an information system.

Security log - A record that contains login and logout activity and other security-related events and that is used to track security issues and information on a computer system.

Security management - Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.

Security posture - The security status of an enterprise — its networks, information, resources, technology, and systems based on information security and assurance resources (i.e., people, hardware, software, and policies). Also, the security posture includes effective security management for the defense of an organization's enterprise when events change and a breach occurs.

Security procedure agreement - An agreement between a financial institution and a Federal Reserve Bank. A financial institution agrees to certain security procedures when using an encrypted communication line with access controls for transmission. These are those receipt and payment order transmissions performed between a financial institution and the Federal Reserve Bank.

Security violation - An instance in which a user or untrusted person circumvents or defeats the controls of a system to obtain unauthorized access to information or system resources.

Segregation of duties - Controls that constitute policies, procedures, and an organizational structure to manage who may control key aspects of computer-related operations.

Sensitive customer information - A customer name, address, or telephone number, in conjunction with the customer social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that may permit access to the customer account. Sensitive customer information also includes any combination of components of customer information that may allow someone to log onto or access the customer account, such as username and password or password and account number.

Server - A computer or other device that manages a network service. An example is a print server, which is a device that manages network printing.

Service provider - May also be referred to as a Technology Service Provider (TSP). Among a broad range of entities, including affiliated entities, non-affiliated entities, and alliances of companies

providing products and services. Other terms used to describe service providers include vendors, subcontractors, external service providers, application service providers, and outsourcing.

Settlement - The final step in the transfer of ownership involving the physical exchange of securities or payment. In a banking transaction, settlement is the process of recording the debit and credit positions of the parties involved in a transfer of funds. In a financial instrument transaction, settlement includes both the transfer of securities by the seller and the payment by the buyer. Settlements can be "gross" or "net." Gross settlement means each transaction is settled individually. Net settlement means parties exchanging payments will offset mutual obligations to deliver identical items (e.g., USD or EURO dollars) at a specified time after which only one net amount of each item is exchanged.

Settlement date (ACH) - The date on which an exchange of funds with respect to an entry is reflected on the books of the Federal Reserve Bank.

Settlement eligible instructions - See "Matched instructions".

Short position - In respect of a currency balance that is less than zero — the amount by which such currency balance is less than zero — an investment position that benefits from a decline in market price. For example, when one sells a currency their position is short.

Short position limit - In respect of an eligible currency — the maximum short position a Settlement Member may have at any time in that eligible currency — unless otherwise reduced pursuant to the CLS Bank Rules — shall equal (i) the total amount of all available committed liquidity facilities in such eligible currency (or such lesser amount that CLS Bank may determine from time to time) minus (ii) the amount of the largest available committed liquidity facility among such liquidity facilities — after taking into account any amounts already drawn.

Significant firms - Firms that process a significant share of transactions in critical financial markets.

Simulated loss of data center site(s) test/exercise - A type of disaster recovery test that involves the simulation of the loss of the primary, alternate, and/or tertiary data processing sites to verify that the institution can continue its data processing activities.

Simulation - The process of operating a model of an enterprise-wide or business line activity in order to test the functionality of the simulation model. Computer systems may support the simulation of business models to aid in evaluating the BCP.

Single-Entry (ACH) - A one-time transfer of funds initiated by an originator in accordance with the receiver's authorization for a single ACH credit or debit to the receiver's consumer account.

SLA - Service Level Agreement. Formal contract between a service provider (i.e., internal or external) and the end user that defines the level of service expected from the service provider. The SLA contract specifies and clarifies performance expectations, establishes accountability, and details consequences if performance or service contract provisions are not met.

Smart cards - A card with an embedded computer chip on which information can be stored and processed.

Sniffing - The passive interception of data transmissions.

Social engineering - A general term for trying to trick people into revealing confidential, personal, and

PII information or performing certain actions.

SONET - Synchronous Optical Network. A standard that defines interface standards for connecting fiber optic (or fibre optic) transmission systems.

Sound practices - Defined in the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," which was issued by the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency and Securities and Exchange Commission.

Source code - Software program instructions written in a format (script or interpreted language) readable by humans.

Source program - A program written in a programming language, such as Basic, C, C++, C#, Pascal, and COBOL. A compiler translates source code into a machine language object program.

Spear phishing - An attack targeting a specific user or group of users with attempts to deceive a user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current user profile information. Sometimes this information is gathered by hacking into the targeted network.

Spiral development - An iterative project management model that focuses on the identification of project and product risks and the selection of project management techniques that best control identified risks.

Split processing - The ongoing operational practice of dividing production processing between two or more geographically dispersed facilities.

Spoofing - A form of masquerading where a trusted IP address is used instead of the true IP address as a means of gaining access to a computer system.

Spot - The most common foreign exchange transaction. Spot or spot date refers to the spot transaction value date that requires settlement within two business days — subject to value date calculation.

SQL Injection Attack - An exploit of target software that constructs structured query language (SQL) statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input — the resulting SQL statement performs actions other than those the application intended. SQL injection enables an attacker to submit code directly to the database bypassing the application completely. A successful injection may cause unauthorized information disclosure as well as ability to add or modify data in the database.

SSL - Secure Sockets Layer. An encryption system developed by Netscape. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. It is used by websites whose referenced site name begins with "https" instead of "http."

Stateful inspection - A firewall inspection technique that examines the claimed purpose of a communication for validity. For example, a communication claiming to respond to a request is compared to a table of outstanding requests.

Storage virtualization - The process of taking many different physical storage networks and devices and

present them as one "virtual" entity for purposes of effective storage management, resource utilization, and administration.

Store card - A credit card issued by a financial institution for a specific merchant or vendor that does not carry a bankcard association logo. Store cards can only be used at the merchant or vendor whose name appears on the front of the card.

Stored-value card - A card-based payment system that assigns a value to a card. A card's value may be stored on the card itself (i.e., on the magnetic stripe or in a computer chip) or in a network database. As the card is used for transactions — the transaction amounts are subtracted from the card's balance. As the balance approaches zero, some cards can be "reloaded" through various methods and others are designed to be discarded. These cards are often used in closed systems for specific types of purchases.

Stovepipe application - Standalone programs that may not easily integrate with other applications or systems.

Street tests - Street tests are also called cross-market tests or market-wide tests that are sponsored by the Securities Industry Association, Bond Market Association, and Futures Industry Association. These tests validate the connectivity from alternate sites and include transaction, settlement, and payment processes to the extent practical.

Substitute check (Check 21) - Also known as the Image Replacement Document (IRD). A paper reproduction of an original check that (1) contains an image of the front and back of the original check; (2) bears a MICR line that, except as provided under ANS X9.100-140, contains all the information appearing on the MICR line of the original check — when it was issued and any additional information that was encoded on the original check's MICR line before an image of the original check was captured; (3) conforms in paper stock, dimension, and otherwise with ANS X9.100-140; and (4) is suitable for automated processing in the same manner as the original check. The Federal Reserve Board of Governors can by rule or order determine different standards.

Sustainability - The period of time for which operations can continue at an alternate processing facility.

SVC - Switched Virtual Circuit. SVC is a temporary connection between workstations that is disabled after communication is complete. Refer to Permanent Virtual Circuit (PVC) for an additional communication method using circuits.

Switch - A device that connects more than two LAN segments that use the same data link and network protocol.

Synchronous data replication - A process for copying data from one source to another in which an acknowledgement of the receipt of data at the copy location is required for application processing to continue. In this way, the content of databases stored in alternate facilities is identical to those at the original storage site and copies of data contain current information at the time of a disruption in processing.

System administration - The process of maintaining, configuring, and operating computer systems.

System resources - Computer capabilities that can be accessed by a user or program either on the users' machine or across the network. (A system resource is any physical or virtual component of limited availability within a computer system. Every device connected to a computer system is a resource.)

T

T-1 line - A special type of telephone line for digital communication and transmission. T-1 lines provide for digital transmission with signaling speed of 1.544Mbps (1,544,000 bits per second). (This is the standard for digital transmissions in North America.)

Tactical plan - A short term plan establishing specific steps needed to implement an organization's strategic plan.

TCO - Total Cost of Ownership. TCO is the purchase price of an asset plus the costs of operation. (The true cost of ownership of a computer or other technology system that includes original cost of the computer and software, license costs and fees, hardware and software upgrades, maintenance, technical support, and training.)

TCP/IP - Transmission Control Protocol/Internet Protocol. A set of protocols and communication standard for transmitting data packets from one computer to another. TCP/IP is used on the Internet (public facing), Intranet (internal facing), and other networks. The two parts of TCP/IP:
Part One. TCP deals with construction of data packets (a.k.a. datagrams) — enables two hosts to establish a connection and exchange streams of data, and;
Part Two. IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.

Technical controls – Security controls that a computer system executes. Technical controls may provide automated protection from unauthorized access or misuse. Technical controls facilitate detection of security violations, issues, threats, and support security requirements for systems, applications, and data. For example, security audit, access controls, and security monitoring tools are technical controls.

Telecommunications - Occurs when exchange of information is between two or more entities (communication) and includes the use of technology to communicate at a distance using electrical signals or electromagnetic waves.

Telnet - An interactive utility, text-based communications session between a client and a host. It is used mainly for remote login and simple control services to systems with limited resources or to systems with limited needs for security.

Terminal services - A component (i.e., utility) of Microsoft Windows operating systems (i.e., both client and server versions known in Windows Server 2008 and earlier) that allows a user to access applications or data stored on a remote computer over a network connection (a.k.a. Remote Desktop Services).

Test assumptions - The concepts underlying an organization's test strategies and plans.

Test key - Internal controls used to verify the authenticity of incoming wire requests involving the use of test keys. A test key is a formula used to develop or interpret test codes or test words. Test codes or words consist of a series of numbers signifying different types of information and usually precede the text of the message. As an example, a test code may contain a bank number, the amount of the transaction, and a number indicating the day and week of the month. As an additional precaution, many test codes contain a variable (sequence number) based on the number of messages received.

Test plan - A document that is based on an organization's test scope and objectives and includes various testing methods.

Test scenario - A potential event, identified as the operating environment for a business continuity or

disaster recovery test, which an organization's recovery and resumption plan may address.

Test scripts - Documents that define the specific activities, tasks, and steps that test participants when conducting the testing process.

Test strategy - Testing strategies establish expectations for individual business lines across the testing life cycle of planning, execution, measurement, reporting, and test process improvement. Testing strategies include the testing scope and objectives, which clearly define what functions, systems, or processes are going to be tested and what will constitute a successful test.

Third party provider - Any type of organization, including affiliated entities, non-affiliated entities, and alliances of companies providing products and services to a financial institution. Other terms used to describe third party providers include subcontractors, external service providers, application service providers, and outsourcers.

Third party relationship - Any business arrangement between an organization and another entity, by contract, agreement, or otherwise.

Third party sender - A special subset of a technology service provider that is authorized to transmit ACH files on behalf of an originator. (The ODFI must rely upon warranties by the third party sender regarding the originators' identity and credit worthiness, which places additional risks on the ODFI.)

Third party service provider - Any type of organization, including affiliated entities, non-affiliated entities, and alliances of companies providing products and services to a financial institution. Other terms used to describe service providers include subcontractors, external service providers, application service providers, and outsourcing.

Threat intelligence - The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance effective decision making.

Token (a.k.a. Security Token) - A small device with an embedded computer chip that can be used to store and transmit electronic information.

Topology - A description of any kind of locality in terms of its physical layout. In the context of communication networks, a topology describes pictorially the configuration or arrangement of a network including its nodes and connecting communication lines.

TPSP - Third Party Service Provider (ACH). A third party, other than the ODFI or RDFI that performs any function on behalf of the ODFI or the RDFI related to ACH processing. Functions may include the creation and sending of ACH files or acting as a sending or receiving point on behalf of a participating depository financial institution.

Transaction testing - A testing activity designed to validate the continuity of business transactions and the replication of associated data.

Trojan horse - Malicious code that is hidden in software, images, or data that appears to be transparent, beneficial, or harmless when referenced or viewed.

Truncating bank (Check 21) - Check 21 gave banks the option of processing checks electronically. The law facilitates check truncation by creating a new negotiable instrument called a substitute check, which permits banks to truncate original checks, to process check information electronically, and to deliver

substitute checks to banks that want to continue receiving paper checks. (A substitute check is the legal equivalent of the original check and includes all the information contained on the original check. The law does not require banks to accept checks in electronic form nor does it require banks to use the new authority granted by the Act to create substitute checks.)

Trusted zone - A channel in which the end points are known and data integrity is protected in transit. Depending upon the communication protocol used — data privacy may be protected in transit. Examples include secure sockets layer (SSL), Internet Protocol Security (IPSec) and its secure physical connection.

TSP – Technology Service Provider. TSPs provide services that make use of current (modern) technology. Examples include Internet service providers (ISPs), web hosting, and technical support organizations (a.k.a. "ITS – Information Technology Services").

Two-way polling - An emergency notification system that allows management to ensure that all employees are contacted and have confirmed delivery of pertinent messages.

U

Ultra forward service - This service allows control over the rerouting of incoming phone calls to predetermined alternate locations in the event of a telecommunications outage.

UPS - Uninterruptible Power Supply. A device that allows your computer to keep running for at least a short time when the primary power source is lost. A UPS may also provide protection from power surges. A UPS contains a battery that "kicks in" when the device senses a loss of power from the primary source allowing the user time to save any data they are working on and to exit before the secondary power source (i.e., the battery) runs out. When a power surge occurs — a UPS intercepts the surge and blocks or minimizes computer or electronic device damage.

URL - Abbreviation for "Uniform (or Universal) Resource Locator." A way of specifying the location of publicly available information on the Internet in the form, "protocol://machine:port number/filename". The port number and/or filename may not be necessary depending upon access requirements.

USA Patriot Act - The USA PATRIOT Act is an Act of Congress "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law Pub.L. 107-56)" — commonly known as the "Patriot Act." The Act was enacted into law by Congress to deter and punish terrorist acts in the United States and around the world. (The law enhances law enforcement investigatory tools of both domestic law enforcement and foreign intelligence agencies.)

US-CERT - The U.S. Computer Emergency Readiness Team is part of the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (US-CERT). The partnership between the Department of Homeland Security and the public and private sectors was established to protect the nation's Internet infrastructure. (US-CERT coordinates defense against and responses to cyber attacks across the nation.)

User identification - The process, control, or information by which a user identifies herself to the system as a valid user (as opposed to authentication).

Utility program - A computer program(s), such as an operating system, performing tasks relating to management of its computer functions, resources, and files — facilitating memory management, password and virus protection plus file compression.

V

VESDA - Very Early Smoke Detection Alert. A system that samples the air on a continuing basis and can detect fire at the precombustion stage.

Virtual machine - A software emulation of a physical computing environment.

Virtual mall - An Internet website offering products and services from multiple vendors or suppliers.

Virus - A malware of malicious code that replicates itself or infects other programs by modifying them within a computer. When a virus replication succeeds, then affected areas are formally identified as "infected."

VLAN - Virtual Local Area Network.

VoIP - Voice over Internet Protocol. The transmission of voice telephone conversations using the Internet or Internet Protocol (IP) networks.

VOIP - Voice Over Internet Protocol. A term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol.

VPN - Virtual Private Network. A computer network that uses public telecommunications infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Vulnerability - A hardware, firmware, or software flaw that leaves an information system open to potential exploitation. A vulnerability weakness may be in automated system security procedures, administrative controls, physical layout, internal controls, etc. It may be exploited to gain unauthorized access to information or to disrupt critical processing.

Vulnerability analysis - Systematic examination of an information system or product. Used to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures. Also, it is used to confirm the adequacy of such measures after implementation.

Vulnerability scanning - Systematic examination of systems to determine the adequacy of security measures, identify security deficiencies, and provide data. Discovery information provided by a scan process is used to predict the effectiveness of proposed security measures.

W

Walk-through drill/simulation test - This test represents a preliminary step in the overall testing process that may be used for training employees, yet not as a preferred testing methodology. (During this drill and simulation test, participants choose a specific scenario and apply the BCP to it.)

Wallet card - Portable information cards that provide emergency communications information for customers and employees.

WAP - Wireless Application Protocol. A data transmission standard to deliver wireless markup language (WML) content.

Warehouse attack - The compromise of systems that store authenticators.

WCAB – Workers' Compensation Appeals Board (California). WCAB exercises all judicial powers vested by the Labor Code in a reasonable and sound manner and provides guidance and leadership to the workers' compensation community through case opinions and regulations. (In the State of Washington, the Board of Industrial Insurance Appeals reviews workers' compensation appeals. The employee, employee's doctor, or employer may appeal a workers' compensation decision to the BIIA, which is an independent agency from the Department of Labor and Industries. The BIIA hears appeals from decisions made by L&I in several areas.)

WEB SEC code - An ACH debit entry initiated by an originator resulting from the receiver's authorization through the Internet to make a transfer of funds from a consumer account of the receiver.

Weblinking - The use of hyperlinks to direct users to webpages of other entities.

Website - A webpage or set of webpages designed, presented, and linked together to form a logical information resource and/or transaction initiation function.

Website hosting - The service of providing ongoing support and monitoring of an Internet-addressable computer that stores webpages and processes transactions initiated over the Internet.

Wide-scale disruption - An event that disrupts business operations in a broad geographic area.

Wireless communication - The transfer of signals from place to place without cables using infrared light or radio waves.

Wireless gateway server - A computer (server) that transmits messages between a computer network and a cellular telephone or other wireless access device.

Wireless phone - See "Mobile device".

WML - Wireless Markup Language. WML is based on XML, it is a markup language intended for devices that implement the Wireless Application Protocol (WAP).

Work program - A series of specific, yet detailed steps to achieve an audit objective.

Work transfer - Work transfer is a process whereby the staff located at a recovery site accepts the workload of staff located at a primary production site. Also, when applicable — a data center located at a recovery site accepts the workload of the primary data processing site.

Workstation - Any computer connected to a local area network.

Worm - A self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (i.e., computers on the network) and it may do so without any user intervention. (A worm is designed to exploit security vulnerabilities on target computers.)

WORM (Acronym) - Write Once, Read Many. A type of optical disk where a computer saves information once to disk and reads saved information many times.

X

XML - Extensible Markup Language is a ”metalanguage” – a language for describing other languages. XML defines a set of rules for encoding documents in a human-readable format. It is designed to improve the functionality of the web by providing more flexible and adaptable information identification.

Z

Zero-day attack - An attack on a piece of software that has a vulnerability for which there is no known patch.

Credit: **Federal Financial Institutions Examination Council**
Note: **The "Glossary of Terminology" is a living document – a glossary that is continually edited and updated.**
Updated: **July 26, 2016**

Modification History

When	Who (Initials)	Why
07/25/2016	BAJ	Added new definition group, which includes: Application security and Data management.
07/26/2016	BAJ	Added pagination feature for break alignment.
