Appendix B: Glossary of Terms

This section contains definitions of terms used within the EBK. A variety of definitions are used by the public and private sectors for each of the key terms and concepts. To work toward a common lexicon for the IT security field, this document presents a glossary that has been developed from the most widely accepted public and private sector sources. For your convenience, some web links have been provided.

Term	Definition
Acceptable Risk	The risk level that an individual or group considers reasonable for the perceived benefit of an activity. Source: United States Coast Guard
Access Card	Often a plastic card with a magnetic strip containing encoded data that is read by passing the card through or over an electronic device, used to provide access to restricted or secure areas. Source: Answers.com
Access Control	Refers first to the practice of restricting entrance to a facility or property to authorized persons, and secondly to the mechanisms which keep track of entries such as visitor's logs, security cameras or prevent access by unauthorized persons through the use of such devices or techniques as gates, electronic locks, biometrics. Source: Merriam Webster's OnLine Dictionary
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
Acquisition	The acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract. Source: Federal Acquisition Regulation (FAR) 2.101
Acquisition Life Cycle	The standard process used by the acquisition organization for defining how a system will be acquired and maintained from inception to retirement. The Acquisition Life Cycle typically follows the waterfall system development model and includes the following phases: Initiation, Planning, Procurement, System Development, System Implementation, Maintenance & Operations, and Closeout. Source: California Office of Systems Integration

Term	Definition
Acquisition Management	Acquisition management is a fully coordinated set of policies, processes, and tools that guide the workforce, both customers and contractors, through the lifecycle process—from the determination of mission needs to the procurement, management, and retirement or replacement of products and services that satisfy those needs. Acquisition management applies monitoring, analysis and measures of performance to the frequently long process of implementing large and complex systems. Source: Innovative Solutions International, Inc.
Aggregation	The ability to get a more complete picture of the information by analyzing several different types of records at once. Source: SANS (SysAdmin, Audit, Network, Security) Institute
Alarm	System consisting of a central controller connected to detection devices, audible warning devices, keypads and controls, power circuitry, and communication devices. Wireless technology has extended the connectivity of traditional hard-wired systems, and IP technology is rapidly changing and extending the description of what was previously a settled and slow-moving domain. A security alarm is typically positioned within the perimeter of physical security, behind the locking hardware. Source: Global Information Assurance Certification (GIAC)
Alternate Facility	A location, other than the normal facility, used to carry out essential functions in a continuity of operations (COOP) situation. Source: Federal Preparedness Circular (FPC) 65
Annual Loss Expectancy (ALE)	The expected monetary loss that can be expected for an asset due to a risk over a one year period. Source: Risky Thinking (www.riskythinking.com)
Annual Rate of Occurrence	The number of times that an organization reasonably expects the risk to occur during one year. Source: Microsoft's Security Risk Management Guide
Anti-Forensic Techniques	Methods used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system. Source: Digital Forensic Research Workshop (DFRWS)
Antivirus Software	Are programs to detect and remove computer viruses. The simplest antiviruses scan executable files and boot blocks for a list of known viruses. Others constantly active, attempting to detect the actions of general classes of viruses. Antivirus software should always include a regular update service allowing it to keep up with the latest viruses as they are released. Source: The Free On-Line Dictionary of Computing
Application Controls	Refer to the transactions and data relating to each computer-based application system and are therefore specific to each such application. The objectives of application controls, which may be manual, or programmed, are to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted. Source: Information Systems Audit and Control Association (ISACA)
Asset Disposal	See Disposal.

Term	Definition
Asset Valuation	The risk management process of determining the monetary value of an asset according to the overall value of the asset to your organization, the immediate financial impact of losing the asset, and the indirect business impact of losing the asset. Source: Microsoft's *Security Risk Management Guide*
Assessment	A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
Auditing	Information gathering and analysis of assets to ensure policy compliance and security from vulnerabilities. Source: SANS Institute
Authentication	The verification of the identity of a person or process. In a communication system, authentication verifies that messages really come from their stated source, like the signature on a (paper) letter. (2001-03-16). Source: The Free On-Line Dictionary of Computing
Authorization	Granting access to a subject to an object after the object has been properly identified and authenticated. Source: Certified Information Systems Security Professional (CISSP), Certification Exam Guide
Awareness (as in Security Training)	A form of security teaching that is a prerequisite to training. The goal of awareness is to bring security to the forefront and make it a recognized entity for users. Source: CISSP, Study Guide
Background Investigation	An inquiry into the background of an individual under consideration for employment, credit, access to sensitive assets (such as national defense information), and other reasons. A background investigation can vary widely from merely checking prior employment experience and educational credentials to civil, criminal, and medical histories. Source: American Society for Industrial Security (ASIS) International
Backup	A spare copy of a file, file system, or other resource for use in the event of failure or loss of the original. The term is most commonly used to refer to a copy of all the files on a computer's disks which is made periodically and kept on magnetic tape or other removable medium (also called a "dump"). Source: The Free On-Line Dictionary of Computing
Backup Strategy	The process that duplicates computer data to offline media, such as magnetic tape. Backups protect data if a system problem should occur. Source: Hewlett-Packard Development Company
Baseline (as in Configuration Management)	Is a set of specifications or work products that has been formally reviewed and agreed on, that thereafter serves as the basic for further development, and that can be changed only through change control procedures. Source: Capability Maturity Model Integration (CMMI), *Guidelines for Process Integration and Product Improvement*
Baseline Security	The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.

Term	Definition
	Source: NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
Benchmarking	Continuous measurement of a process, product, or service compared to those of the toughest competitor, to those considered industry leaders, or to similar activities in the organization in order to find and implement ways to improve it. Source: Joint Commission on Accreditation of Healthcare Organizations (JCAHO)
Biometrics	The science and technology of measuring and statistically analyzing biological data. In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes. Source: Merriam Webster's OnLine Dictionary
Bit-Stream Copy/Image	The technical term for the end-product of a forensics acquisition of a computer's hard drive. The bit-stream copy is much more thorough than a standard back-up or mirror image of a hard drive. The bit-stream copy involves the copying of every bit of data on an "evidence" hard drive, which includes the file slack, and unallocated file space in which deleted files and e-mails are frequently recovered from. Source: CyberControls, LLC
Budget Process and Financial Management	Budget Process: The procedures whereby decisions are made on the allocation and use of funds and such uses are recorded and checked over a budget cycle. Financial Management: A set of tools to support the achievement of budget management objectives, usually by linking budget planning, execution, accounting and monitoring. Source: National Association of State Budget Officers (NASBO)
Built-in Security	The integration of security principles, policies, and procedures into all system development life cycle processes. Source: Essential Body of Knowledge
Business Continuity Plan	Plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Source: SANS Institute
Business Impact Analysis (BIA)	An analysis of an IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. Source: NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*
Business Recovery Plan (BRP)	The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred. Source: NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*
Capital Planning	Capital Planning is a systematic approach to managing the risks and returns of IT investments for a given mission. Source: CIO Council Committees on Capital Planning
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which

Term	Definition
	the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
Certification (as in Training)	The awarding of a credential acknowledging that an individual has demonstrated proof of a minimum level of knowledge or competence, as defined by a professional standards organization. Professional certification can be used as a screening tool and verification of an individual's skills and knowledge. Source: American Society for Training and Development (ASTD)
Chain of Custody	The movement and location of real evidence, and the history of those persons who had it in their custody, from the time it is obtained to the time it is presented in court. Source: Black's Law Dictionary, Eighth Edition
Cluster (architecture)	Multiple servers providing the same service. The term may imply resilience to failure and/or some kind of load balancing between the servers. (1996-11-04). Source: The Free On-Line Dictionary of Computing
Cluster (file system)	An elementary unit of allocation of a disk made up of one or more physical blocks. A file is made up of a whole number of possibly non-contiguous clusters. The cluster size is a tradeoff between space efficiency (the bigger is the cluster, the bigger is on the average the wasted space at the end of each file) and the length of the File Allocation Table. (1996-11-04). Source: The Free On-Line Dictionary of Computing
Communications Security (COMSEC)	Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. Source: Information Assurance Program, Idaho State University
Compliance	The act of conforming, submitting, or adapting to a regulation. Source: Merriam Webster's Online Dictionary
Computer-Based Training	Computer-based training (CBT) is any course of instruction whose primary means of delivery is a computer. A CBT course (sometimes called courseware) may be delivered via a software product installed on a single computer, through a corporate or educational intranet, or over the Internet as Web-based training. Source: TechTarget.com
Computer Forensics	Computer forensics, also called cyberforensics, is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it. Source: SearchSecurity.com
Computer Security	The protection of data and resources from accidental or malicious acts, usually by taking appropriate actions. These acts may be loss or unauthorized modification, destruction, access, disclosure, or acquisition.

Term	Definition
	Source: American National Standard Dictionary of Information Technology (ANSDIT)
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
Configuration	The manner in which the hardware, software, or other aspects of an information processing system are organized and interconnected. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Configuration Management	The management of changes made to a MIS hardware, software, firmware, documentation, tests, test fixtures, test documentation, communications interfaces, operating procedures, installation structures, and all changes thereto throughout the development and operational life-cycle of the MIS. Source: Cyber Security and Critical Infrastructure Coordination
Contract	An agreement between two or more parties creating obligations that are enforceable or otherwise recognized at law. The writing that sets forth such an agreement. A contract is valid if under the law of the residence of the party wishing to enforce the contract. Source: Black's Law Dictionary, Eighth Edition
Copy/Image	To image a hard drive is to make an identical copy of the hard drive, including empty sectors. Also known as creating a "mirror image" or "mirroring" the drive. Source: American Document Management
Cost-benefit Analysis	A cost benefit analysis is done to determine how well, or how poorly, a planned action will turn out. Although a cost benefit analysis can be used for almost anything, it is most commonly done on financial questions. Since the cost benefit analysis relies on the addition of positive factors and the subtraction of negative ones to determine a net result, it is also known as running the numbers. Source: About, Inc. (www.about.com)
Crisis Communications	Refers to communication about an unfortunate event or occurrence that can hurt people, organizations, and economies, among other things. Source: CNET Networks
Cryptosecurity	The IT security discipline that embodies the principles means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. Source: NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*
Curriculum	The courses offered by an educational institution or a set of courses constituting an area of specialization. Source: Merriam Webster's Online Dictionary
Cyber Incident Response	A way to minimize possible impacts of cyber security incidents and assist in the identification, classification, response, and reporting of cyber security incidents related to critical cyber assets. Source: Information Sharing and Analysis Center
Cyber Law	The field of law dealing with the Internet, encompassing cases, statutes, regulations, and disputes

Term	Definition
	that affect people and business interacting through computers. Source: Black's Law Dictionary, Eighth Edition
Data Classification	The conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled and secured and is also indicative of its value in terms of business assets. Source: Information Security Policy and Disaster Recovery Associates
Decryption	The process of transforming ciphertext into plaintext. Source: NIST SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
Defense-in-depth	Defense in depth is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. Source: SANS Institute
Delegation of Authority	The act of pre-delegating authorities for making policy determinations and decisions at headquarters, field levels, and other organizational locations, as appropriate to ensure rapid response to any emergency situation requiring Continuity of Operation Plan implementation. Source: Federal Preparedness Circular (FPC) 65
Digital Forensics	The field of study encompasses not just digital evidence, but also the areas of cyber law, sociology, and security to name a few. Its increasing importance is reflected in its growing role within crime investigations, civil cases and homeland security. Source: Conference on Digital Forensics, Security and Law
Digital Forensics Systems	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. Source: NIST SP 800-61, *Computer Security Incident Handling Guide*
Digital Identity	The electronic representation of a real-world entity. The term is usually taken to mean the online equivalent of an individual human being, which participates in electronic transactions on behalf of the person in question. However a broader definition also assigns digital identities to organizations, companies and even individual electronic devices. Various complex questions of privacy, ownership and security surround the issue of digital identity. Source: LooselyCoupled.com
Digital Signature	A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission. Source: SANS Institute
Disaster Recovery	Disaster Recovery is the process of recovery of IT systems in the event of a disruption or disaster. Source: SANS Institute
Discretionary Access Control	A means of optionally restricting access to objects, based on the identity of subjects, the groups to which they belong, or both of these criteria. Access controls are discretionary in the sense that a subject with a particular access right can pass that access to any other subject. Contrast with mandatory access control, need-to-know.

Term	Definition
	Source: American National Standard Dictionary of Information Technology (ANSDIT)
Disk File System	A set of instructions or data that is recorded, cataloged and treated as a single unit on a disk. Source language programs, machine language programs, spreadsheets, data files, text documents, graphics files and batch files are examples. Source: PCMag.com
Disposal	The act or process of getting rid of something. Regency Technologies, LLC
Disruption	A disordering or confusion. An interruption or impediment to the usual course of activity. Source: Webster's II New College Dictionary
Duplicate Image	An accurate digital reproduction of all data objects contained on the original physical item and associated media. Source: NIST SP 800-72, *Guidelines on PDA Forensics*
e-discovery	Electronic discovery (also called e-discovery or ediscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network. Court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery. Source: SearchFinancialSecurity.com
Electronic Commerce	Commerce conducted via the internet. Source: Merriam Webster's Online Dictionary
Emission Security	Protection against compromising emanations. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Encryption	The cryptographic transformation of data. The result of encryption is ciphertext. The reverse process is called decryption. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Encryption Technologies	Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used. Source: SANS Institute
End User Security Training	In information technology, the term end user is used to distinguish the person for whom a hardware or software product is designed from the developers, installers, and servicers of the product. Source: TechTarget.com
Enterprise Architecture	An enterprise architecture (EA) is a conceptual blueprint that defines the structure and operation of an organization. The intent of an enterprise architecture is to determine how an organization can most effectively achieve its current and future objectives. Source: SearchCIO.com
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.

Term	Definition
	Source: The Committee of National Security Systems (CNSS) Inst. 4009, Revised June 2006, National Information Assurance (IA) Glossary
Environmental Threat	Any natural event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets (including information systems), or individuals.. Source: Essential Body of Knowledge
Escalation Procedures	The procedures used to increase in extent, volume, number, amount, intensity, or scope of a service request to resolve an IT security issue. Source: Essential Body of Knowledge
Essential Functions	Functions that enable enterprises to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain the industrial/economic base in an emergency. Source: Federal Preparedness Circular (FPC) 65
Ethics	The discipline dealing with what is good and bad and with moral duty and obligation. Source: Merriam Webster's Online Dictionary
Evaluation	Evaluation is the systematic collection and analysis of data needed to make decisions, a process in which most well-run programs engage from the outset. Source: Evaluation.wiki.com
Evidence Archival	Information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats. Source: LuciData.com
Firewall	A functional unit that mediates all traffic between two computer networks and protects one of them or some part thereof against unauthorized access. The protected network is in general a private, internal network. A firewall may permit messages or files to be transferred to a high-security workstation within the internal network, without permitting such transfer in the opposite direction. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Firewall Configuration	A firewall configuration (ruleset) is a table of instructions that the firewall uses for determining how packets should be routed between its interfaces. In routers, the ruleset can be a file that the router examines from top to bottom when making routing decisions. Source: NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*
Forensic Analysis	A medical, chemical, toxicological, ballistic, information system, or other expert examination or test performed on physical evidence including DNA evidence, for the purpose of determining the connection of the evidence to a criminal action. Source: Forensic Laboratory Advisory Board
Forensic Labs	A highly specialized facility that provides forensic examinations of digital media, such as computers, in support of investigations and/or prosecutions.

Term	Definition
	Source: C.E. Cantwell and Associates, Inc.
Governance	The act, process, or power of government. Source: Webster's II New College Dictionary
Hub	In distributed systems, a functional unit that provides interconnectivity between multiple nodes. Hubs may be passive or include repeaters but do not provide switching or routing. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Human Resources	The function dealing with the management of people employed within the organization. Source: Society for Human Resource Management
Identification and Authentication	In computer security, the process that enables recognition of an entity by a system, through personal, equipment, or organizational characteristics or codes. Authentication in security, the act of verifying the claimed identity of an entity. Source: American National Standard Dictionary - Information Technology
Identity Data and Access Management	Processes, technologies, and policies to manage digital identities and specify how they are used to access resources. Source: Microsoft Corporation
Identity Management	The comprehensive management and administration of user permissions, privileges, and individual profile data. It provides a single point of administration for managing the lifecycle of accounts and profile data. Source: Meta Access Management System (MAMS), Federated Identity and Access Management Glossary
Incident Handling	The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61, *Computer Security Incident Handling Guide*
Incident Records	Records containing the details and history of an incident. Source: IT Infrastructure Library (ITIL)
Incident Response	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT systems(s). Source: NIST SP 800-34, *Contingency Planning Guide for Information Technology (IT) Systems*
Information Assurance Posture	Physical and technical assessment of the organization's threats, vulnerabilities, countermeasures, and risks. Source: Information Assurance, A Practical Guide (James Boyce)
Information Classification Scheme	A classification scheme is the descriptive information for an arrangement or division of objects into groups based on characteristics, which the objects have in common. Source: OECD Glossary of Statistical Terms
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. Source: CNSS Inst. 4009, National Information Assurance (IA) Glossary
Information	Stakeholders are the specific people or groups who have a stake, or an interest, in the outcome of

Term	Definition
Stakeholder	the project. Normally stakeholders are from within the company, and could include internal clients, management, employees, and administrators. Source: Visitask.com
Information System	An information processing system together with associated organizational resources such as human, technical, and financial resources, that provides and distributes information. In databases, the conceptual schema, information base, and information processor, forming together a system for keeping and manipulating information. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Information Technology Contingency Plan	A set of advanced arrangements and procedures that define interim measures that enable an organization to respond to incidents and restore mission critical services or operations following a disruptive event. Source: NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*
Insider Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. Source: NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*
Instructional Systems Design (ISD)	An organized procedure for developing instructional materials programs, or curricula; includes the steps of analyzing, designing, developing, implementing, and evaluating. Source: Glossary of Instructional Design Terminology
Instructor Led Training (ILT)	Also known as Instructor Based Training (IBT), this method is closest to that of a traditional classroom experience. In an ILT, the electronic components supplement and enhance traditional teaching methods. The strength of an ILT is collaboration because participants interact, provide feedback, and ask questions for quick and effective learning. In addition to the course content, an ILT contains tips for the instructor. Typical components of an ILT are Student Guide, Instructor Guide, and Microsoft PowerPoint slides. Source: Elliott Masie's Learningwiki.com
Instructional Systems Design	A formal process for designing training, be it computer-based or traditional instructor-led training. The ISD process includes analysis, design, development, implementation, and evaluation. Also known as System Approach to Training (SAT). Source: Northeastern Illinois University
Integrity of Evidence	The isolation of a computer system so evidence will not be lost. Source: Governmentsecurity.org
Interoperable Communications	Alternate communications that provide the capability to perform essential functions, in conjunction with other agencies, until normal operations can be resumed. Source: Federal Preparedness Circular (FPC) 65
Intrusion	Unauthorized access to a computer system or network. Source: TechEncyclopedia.com
Intrusion Detection System	A system to detect, report, and provide limited response to an activity that may be harmful to an information system.

Term	Definition
	Source: SANS Institute
Intrusion Prevention System	Used in computer security. It provides policies and rules for network traffic along with an intrusion detection system for alerting system or network administrators to suspicious traffic, but allows the administrator to provide preventive action upon being alerted. Some compare it to a combination of Intrusion Detection Systems and an application layer firewall for protection. Source: Webopedia.com
Inventory	A detailed list of items in one's view or possession; a periodic survey of all goods and materials in stock.. Source: Webster's II New College Dictionary
IT-Related Risk	The net mission impact considering, 1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and 2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to: 1. Unauthorized (malicious or accidental) disclosure, modification or destruction of information; 2. Unintentional errors and omissions; 3. IT disruptions due to natural or man-made disasters; 4. Failure to exercise due care and diligence in the implementation and operation of the IT system. Source: NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
Job Rotation	Rotating employees among various job positions. It provides a type of knowledge redundancy and reduces the risk of fraud, data modification, etc. Source: CISSP Study Guide
Laws	A binding custom or practice of a community; a rule of conduct or action prescribed or formally recognized as binding or enforced by a controlling authority. Source: Merriam Webster's Online Dictionary
Learning Management System (LMS)	A program that manages the administration of training. Typically includes functionality for course catalogs, launching courses, registering students, tracking student progress and assessments. Source: e-LearningGuru.com
Learning Objectives	A statement establishing a measurable behavioral outcome, used as an advanced organizer to indicate how the learner's acquisition of skills and knowledge is being measured. Source: American Society for Training and Development (ASTD)
Least Privilege	The security principle that requires each subject to be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. Source: CISSP, Certification Exam Guide
Likelihood Determination	Rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment based on factors such as threat-source motivation and capability, nature of the vulnerability, and the existence and effectiveness of current controls. Source: NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
Load Balancers	The fine tuning of a computer system, network or disk subsystem in order to more evenly distribute the data and/or processing across available resources. For example, in clustering, load balancing might distribute the incoming transactions evenly to all servers, or it might redirect

Term	Definition
	them to the next available server. Source: PCMag.com
Mandatory Access Control	A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. Source: NIST SP 800-44, *Guidelines on Securing Public Web Servers*
Manmade Threat	An expression of intention to inflict evil, injury, or damage that is manufactured, created, or constructed by human beings. Manmade threats may involve devastating acts using weapons of mass destruction ranging from chemical agents, biological hazards, a radiological or nuclear device, and other explosives. Source: ReadyOC.org
Measures	See Security Measures.
Mission Assurance	An engineering process performed over the life cycle of a program to identify and mitigate design, production, test, and field support deficiencies that could affect mission success. It requires the application of system engineering, risk management, quality and management principles to achieve mission success. It relies on independent technical assessment throughout the entire design, development, testing, deployment, and operations process. Source: Grimm, John. (November 16, 2004). *The Role of CMMI in Mission Assurance*.
Natural Threat	An indication of something impending from the external world in its entirety. Examples of natural threats include floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events. Source: Merriam Webster's Online Dictionary
Need-To-Know	A legitimate requirement of a prospective recipient of data to know, to access, or to possess any sensitive information represented by these data. A determination that a prospective recipient of sensitive information has a legitimate requirement to access, to have knowledge of, or to possess that information. Contrast with clearance, discretionary access control. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Needs Assessment	A needs assessment is an evaluation of the technical tasks and functions an organization must be capable of performing (that it currently isn't) or the needs that technology must be able to meet (that are not currently being met). A true needs assessment requires that all possible needs be identified. Determining whether they are realistic, and affordable comes at a later point in the planning process. Source: National Center for Education Statistics (NCES)
Network Architecture	A set of design principles, including the organization of functions and the description of data formats and procedures, used as the basis for the design and implementation of a network. Source: International Organization for Standardization (ISO)
Network Forensics	See Digital Forensics.
Networking Models and Protocols	Networking models such as the OSI Reference Model provide a framework for breaking down complex internet works into components that can more easily be understood and utilized. The

Term	Definition
	model defines networking functions not as a large, complicated whole, but as a set of layered modular components, each of which is responsible for a particular function. The result is better comprehension of network operations, improved performance and functionality, easier design and development, and the ability to combine different components in the way best suited to the needs of the network. Source: The TCP/IP Guide – The Benefits of Networking Models
Network Monitoring	Collects, visualizes, and archives flow records from its sensors for the monitoring and enforcement of use policies. Source: Institute for Secure Information Systems
Network Segmentation	The act or profession of splitting a computer network into subnetworks, each being a network segment or network layer. Advantages of such splitting are primarily for boosting performance and improving security. Source: Wikipedia.com
Nondisclosure Agreement	A contract or contractual promise containing a person's promise not to disclose any information shared by or discovered from a trade-secret holder, including all information about trade secrets, procedures, or other internal matters. Source: Black's Law Dictionary, Eighth Edition
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
Occupant Emergency Plan	An occupant emergency is an event that threatens life and property in specific occupied space. An Occupant Emergency Plan is designed to protect both employees assigned to the building/facility and visitors. An emergency may involve fires, bomb threats, explosions, HAZMAT, demonstrations, civil disturbances, hostage situations, floods, hurricanes, winter storms, tornadoes, power failures, earthquakes, as well as other natural and human caused disasters. Source: Internal Revenue Service, Internal Revenue Manual, Occupant Emergency Plan
Order of Succession	A protocol to the act or right of legally or officially taking over a predecessor's office, rank, or dutied. Source: Black's Law Dictionary, Eighth Edition
Patch Management	A process for identifying, testing, installing, and monitoring compliance with software patches. Source: EDUCAUSE
Penetration Testing	Examining the functions of a data processing systems to find a means of circumventing computer security. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Performance Management	Performance management is the systematic process by which the organization involves its employees, as individuals and members of a group, in improving organizational effectiveness to accomplish the organization's mission and goals. Source: Internal Revenue Service, Internal Revenue Manual, Human Resource Management: Performance Management

Term	Definition
Perimeter Defense	An IT security defense method that integrates security at all layers of the architecture, including router, switch, network, operating system, file system, database, and applications layers. Source: Microsoft Corporation
Persistent Data	Data that exists from session to session. Persistent data are stored in a database on disk or tape. Source: PC Magazine (PCMag.com)
Personally Identifiable Information (PII)	Any information relating to an identified or identifiable individual. Such information may include name, country, street address, e-mail address, credit card number, Social Security number, government ID number, IP address, or any unique identifier that is associated with PII in another system. Also known as personal information or personal data. Source: Microsoft Corporation
Policy	The general principles by which a government is guided in its management of public affairs. Source: Black's Law Dictionary
Port	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows. Source: FIPS 140-2, *Security Requirements for Cryptographic Modules*
Portable Media Forensics	The physical material used to store electronic data. Portable media includes computer disks, CD, DVD, PDA memory, disaster recovery tapes, etc. Source: American Document Management
Position Sensitivity	Determines the type of security investigation required before individuals can be assigned to sensitive positions and granted the applicable clearance level (e.g., secret, top secret, etc.). There are four types of sensitivity designations: Nonsensitive - position involves access to unclassified information - requires National Agency Check investigation; Noncritical Sensitive - position involves access to confidential or secret information - requires National Agency Check and credit investigation; Critical Sensitive - position involves access to top secret information - requires full background investigation; Special Sensitive - position involves access to top secret/sensitive compartmented information - requires full background investigation. Source: U.S. Army
Preparedness/ Readiness	The state of being ready in advance of a particular purpose, event, or occasion. Source: Webster's II New College Dictionary
Prequalification	The screening of potential vendors in which such factors as financial capability, reputation, and management are considered when developing a list of qualified vendors. Source: State of Minnesota Materials Management Division
Privacy Principles	Eleven principles that outline the legal requirements of privacy in electronic communications are: Principle 1 - Manner and purpose of collection of personal information Principle 2 - Solicitation of personal information from individual concerned Principle 3 - Solicitation of personal information generally Principle 4 - Storage and security of personal information

Term	Definition
	Principle 5 - Information relating to records kept by record-keeper Principle 6 - Access to records containing personal information Principle 7 - Alteration of records containing personal information Principle 8 - Record-keeper to check accuracy etc of personal information before use Principle 9 - Personal information to be used only for relevant purposes Principle 10 - Limits on use of personal information Principle 11 – Limits on disclosure of personal information Source: Information Privacy Principles under the Privacy Act 1988
Privilege Levels / Accounts	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts. Source: NIST SP 800-12, *An Introduction to Computer Security*
Procedure	Established or prescribed methods to be followed routinely for the performance of designated operations or in designated situations. Source: Merriam Webster's Online Dictionary
Process Maturity	The extent to which a specific process is explicitly defined, managed, measured, controlled, and implemented effectively. Maturity implies a potential for growth in capability and indicates the sophistication of an organization's processes and the consistency with which the organization conducts these processes. Source: Information Technology Investment Management, A Framework for Assessing and Improving Process Maturity
Public Key Infrastructure	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. Source: CNSS Inst. 4009, Revised June 2006, National Information Assurance (IA) Glossary
Reconstitution of System	Implemented after the recovery phase, reconstitution procedures are carried out to restore the original facility and IT system to normal operating conditions. If use of the original site or system is not feasible as a result of extensive damage, actions should be taken during reconstitution to procure and prepare a new facility or IT system. When the original or new site and system are ready, recovery activities are terminated, and normal operations are transferred back to the organization's. Source: NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*
Regulations	Rules and administrative codes issued by governmental agencies at all levels, municipal, county, state and federal. They have the force of law, since they are adopted under authority granted by statutes, and often include penalties for violations. Source: LegalDictionary.com
Regulatory Compliance	Compliance is either a state of being in accordance with established guidelines, specifications, or legislation or the process of becoming so. Source: Bitpipe.com
Request for Information	A document used to obtain price, delivery, other market information, or capabilities for planning purposes when the Government does not presently intend to issue a solicitation.

Term	Definition
	Source: FAR 15.202(e)
Request for Proposal (RFP)	A solicitation for offers under negotiation procedures. Source: Glossary of Acquisition Terms, Federal Acquisition Institute
Residual Risk	The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. Source: NIST SP 800-16, Appendix C – Glossary, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
Risk	See IT-Related Risk.
Risk Analysis	A systematic method of identifying the assets of a data processing system, the threats to those assets, and the vulnerability of the system to those threats. Synonymous with risk assessment. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Risk Assessment	Synonym for risk analysis. A systematic method of identifying the assets of a data processing system, the threats to those assets, and the vulnerability of the system to those threats. Synonymous with risk assessment. Source: American National Standard Dictionary of Information Technology (ANSDIT)
Risk-Based Decision	An approach to regulatory decision making in which such decisions are made solely based on the results of a probabilistic risk analysis. Source: U.S. Nuclear Regulatory Commission
Risk Level	The combined result of consequence and probability. Source: Business Continuity Institute
Risk Management	The total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws. Source: NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
Risk Mitigation	Risk mitigation encompasses loss prevention, loss control, and claims management. Structured effectively, a risk mitigation program will prevent losses and reduce the cost of losses that do occur while creating a safer environment for your employees, your business partners, and the communities in which you operate. Source: Aon Corporation
Role-Based Access Control	The privilege to use computer information in some manner based upon an individual's role. Source: Webopedia
Role-Based Training	Training designed and delivered based on the set of functions performed and work products or deliverables owned in an organization. Source: Essential Body of Knowledge
Router	A functional unit that establishes a path through one or more computer networks. In computer networks conforming to the OSI model, a router operates at the network layer.

Term	Definition
	Source: American National Standard Dictionary of Information Technology (ANSDIT)
Rule Based Access Control	A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. Source: NIST SP 800-33, *Underlying Technical Models for Information Technology Security*
Secure Coding	Secure Coding works with software developers and software development organizations to reduce vulnerabilities resulting from coding errors before they are deployed. Secure coding identifies common programming errors that lead to software vulnerabilities, establishes standard secure coding standards, educates software developers, and advances the state of the practice in secure coding. SOURCE: Software Engineering Institute, Carnegie Mellon University
Secure Coding Principles	Secure Coding Principles are: Minimize attack surface area; Establish secure defaults; Principle of least privilege; Principle of defense in depth; Fail securely; Don't trust services; Separation of duties; Avoid security by obscurity; Keep security simple; Fix security issues correctly. Source: Open Web Application Security Project
Secure Coding Tools	Categories of such tools include: Static Code Checkers; Runtime Code Checkers; Profiling Tools; Penetrations Testing Tools; Application Scanning Tools. Source: Secure Coding: Principles and Practices
Secure Data Handling	Procedures put in place to prevent distribution of information to third parties or online posting of information. Source: Department of Ethics and Consumer Affairs
Security Alerts	Advisory that an emergency situation has either occurred or is approaching, but is less imminent than implied by a warning message. Source: Virginia Radio Amateur Civil Emergency Service (RACES)
Security Audit	A systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria. Source: TechTarget.com
Security Breach	A breach of security is where a stated organizational policy or legal requirement regarding Information Security, has been contravened. However every incident which suggests that the Confidentiality, Integrity and Availability of the information has been inappropriately changed, can be considered a Security Incident. Every Security Breach will always be initiated via a Security Incident, only if confirmed does it become a security breach. Source: YourWindowTo.com.
Security Change Management	Is a process to ensure all changes that impact the security posture of an enterprise are reviewed, tracked, documented, and approved in terms of their efficacy to meet security requirements and government regulations. Source: Essential Body of Knowledge
Security Clearance	Permission granted to an individual to access information at or below a particular security level. Synonymous with clearance.

Term	Definition
	Source: American National Standard Dictionary of Information Technology (ANSDIT)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Source: FIPS 199, *Recommended Security Controls for Federal Information Systems*
Security Data Analysis	The ability to obtain information from data by detecting anomalies at low concentrations with minimal level of false positives and negatives Source: American Society of Civil Engineers: Candidate Instruments and Observables
Security Incident	An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event. Source: SANS Institute
Security Measures	Measures taken as a precaution against theft or espionage or sabotage, etc. Source**:** TheFreeDictionary.com
Security Program	The encapsulation of an organization's security strategy. This generally includes: Security Office Mission and Mandate; Security Office Governance; Security Policy Development and Management; Security Training and Awareness Development; and Security Project Portfolio Development. Source: CISO/CSO Handbook
Security Reporting	Presenting data to internal management and external users such as regulators, shareholders, the general public, and specific stakeholder groups. Source: World Resources Institute
Security Requirements	Types and levels of protection necessary for equipment, data, information, applications, and facilities. Source: Texas State Library and Archives Commission
Security Requirements Analysis	An analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required. Source: NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*
Security Specifications	Detailed description of the safeguards required to protect an IS. Source: CNSS Inst. 4009, Revised 2006, National Information Assurance (IA) Glossary
Security Testing and Evaluation	An examination or analysis of the protective measures that are placed on an information system once it is fully integrated and operational. The objectives of the security testing and evaluation are to: • uncover design, implementation and operational flaws that could allow the violation of security policy • determine the adequacy of security mechanisms, assurances and other properties to

Term	Definition
	enforce the security policy • assess the degree of consistency between the system documentation and its implementation. Source: NIST SP 800-42, *Guideline on Network Security Testing*
Security Trust	See Trust Level.
Security Vulnerability Analysis	Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use. Source: Searchsecurity.com
Sensitive Information	As defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives. Source: SANS Institute
Sensitivity Determination	A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted. Source: FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*
Sensitivity of Data	The need to protect data from unauthorized disclosure, fraud, waste or abuse. Source: The Center for Information Technology, National Institutes of Health
Separation of Duties	A security principle that says no one person should be able to affect a breach of security. For example, the person who writes a check should not be the one to sign it. Separation of duties requires that people who make changes in production source code hand off their changes to someone else for installation control. Separation of duties forces rogue employees into attempting collusion and thus risking discovery by honest coworkers. Source: PCMAG.com
Service Level Agreement (SLA)	Contractual agreements between entities describing specified levels of service that the servicing entity agrees to guarantee for the customer. Source: *Security+ Certification All-In-One Exam Guide*
Single Loss Expectancy	The total amount of revenue that is lost from a single occurrence of the risk. It is a monetary amount that is assigned to a single event that represents the company's potential loss amount if a specific threat exploits vulnerability. Source: Microsoft's Security Risk Management Guide
Social Engineering	A non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. Source: TechTarget.com
Software Assurance	The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner. Source: CNSS Inst. 4009, Revised June 2006, National Information Assurance (IA) Glossary
Solicitation	1. A document sent to prospective contractors by a Government agency requesting submission of

Term	Definition
	an offer, quote, or information. 2. The process of issuing a document requesting submission of an offer, quote, or information and obtaining responses. Source: Glossary of Acquisition Terms, Federal Acquisition Institute
Special Background Investigation	A Special Background Investigation (SBI) is the minimum investigative requirement for access to Sensitive Compartmented Information (SCI) or for participation in certain other Special Access Required (SAR) and Extremely Sensitive Information programs. The SBI consists of all components of a traditional Background Investigation (BI), plus specific additional investigative requirements. The period of investigation for SBIs covers the last 15 years of the subject's life or from the date of the 18th birthday, whichever was the shorter period, provided that the period covers at least the last 2 full years (but does not precede the 16th birthday). Source: Federation of American Scientists
Standards	Establish measurable controls and requirements to achieve policy objectives. Source: Federal Financial Institutions Examination Council
Standard Operating Procedure	A prescribed written procedure outlining how recurring tasks, duties and functions are to be performed organization-wide. Source: Society for Human Resource Management
Statement of Objectives (SOO)	Expresses both technical and management requirements in the form of performance objectives. In these cases, the offerors are expected to prepare the Statement Of Work (SOW) in response to the SOO. Source: Acquisition Strategy Decision Guide, Department of the Navy
Statement of Work (SOW)	A detailed pragmatic statement of a company's needs and requirements on which prospective suppliers base their bids or proposals to provide products or services. Source: Society for Human Resource Management
Steganography	The act of embedding messages within another message such that the message is hidden from common view. Source: CISSP Study Guide
Strategic Planning	Strategic planning is the process by which an organization envisions its future and develops strategies, goals, objectives and action plans to achieve that future. Source: Visitask.com
Strategic Resource and Investment Management	The management of a specified appropriation or its subdivision, revolving fund, or for the management of the overall manpower authorization. Source: Defense Acquisition University
Suitability Determination	Suitability refers to identifiable character traits and past conduct which are sufficient to determine whether an individual is likely or unlikely to be able to carry out the duties of the job with appropriate efficiency and effectiveness. It also refers to statutory or regulatory bars which prevent the lawful employment of the individual into the position. Source: Department of the Interior
Switch	A networking device that keeps track of MAC addresses attached to each of its ports so that data

Term	Definition
	is only transmitted on the ports that are the intended recipient of the data. Source: SANS Institute
System Compromise	Involves increased access beyond authorization, information disclosure, and resource theft. Source: Your Dictionary.com
System Development Life Cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. Source: NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*
System Engineering	The design of a complex interrelation of many elements (a system) to maximize an agreed-upon measure of system performance, taking into consideration all of the elements related in any way to the system, including utilization of worker power as well as the characteristics of each of the system's components. Source: McGraw Hill, Sci-Tech Dictionary
System Hardening	The purpose of system hardening is to eliminate as many security risks as possible. This is typically done by removing all non-essential software programs and utilities from the computer. While these programs may offer useful features to the user, if they provide "back-door" access to the system, they must be removed during system hardening. Source: TechTerms.com
System Logs	A file that lists actions that have occurred. Source: Webopedia.com
System Monitoring	See Network Monitoring.
System of Records	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Source: The Privacy Act of 1974, 5 U.S.C. Sec. 552a
Technical Security Controls	Technical controls use technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Technical controls are far-reaching in scope and encompass such technologies as Encryption, Smart cards, Network authentication, Access control lists (ACLSs), and File integrity auditing software. Source: Red Hat, Inc.
Telecommunications Technology	Electronic or digital products and systems for all types of data transmission, from voice to video. Source: Webopedia.com
Testing (as in Training)	A series of questions, problems, or physical responses designed to determine knowledge, skills, or ability. Source: Answers.com
Test, Training and Exercise (TT&E) Plan	A Plan that outlines the steps to be taken to ensure that personnel are trained in their IT plan roles and responsibilities, IT plans are exercised to validate their viability, and IT components or systems are tested to validate their operability in the context of an IT plan.

Term	Definition
	Source: NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. [CNSS Instruction 4009 Adapted] Source: CNSS Inst. 4009, Revised June 2006, National Information Assurance (IA) Glossary
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment. Source: NIST SP 800-27A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*
Threat Environment	An area that contains known threats and possesses little or no control over the surrounding area. Source: Air Force Regulation 205-16
Threat Modeling	A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability. Source: SANS Institute
Threat Monitoring	See Network Monitoring.
Threat Motivation	The relative amount of incentive that a threat has to compromise or damage the assets of an organization. Source: Symantec
Total Cost of Ownership	A comprehensive assessment of information technology (IT) or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses, and the opportunity cost of downtime, training and other productivity losses. Source: Gartner, Inc.
Training	A process that aims to improve knowledge, skills, attitudes, and/or behaviors in a person to accomplish a specific job task or goal. Training is often focused on business needs and driven by time-critical business skills and knowledge, and its goal is often to improve performance. Source: American Society for Training and Development (ASTD)
Transmission Security	All measures designed to protect transmission from interception, traffic analysis, and imitative deception. Source: Integrated Publishing, Electrical Engineering Training Series
Trust Level	Tells the customer how much he/she can expect out of this system, what level of security it will provide, and the assurance that the system will act in a correct and predictable manner in each and every computing situation. Source: CISSP Certification Exam Guide
Types of Risk	The possibility of loss resulting from a threat, security incident, or event.

Term	Definition
	Source: ASIS International
Unauthorized Access	Approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without consent. Source: National Conference of State Legislatures
User Privileges	The authorization given to users that enables them to access specific resources on the network, such as data files, applications, printers and scanners. User permissions also designate the type of access; for example, can data only be viewed (read only) or can they be updated (read/write). Source: PCMag.com
User Provisioning	A procedure for enabling end users to access and use system services. Provisioning involves creating for each end user an account in a directory service and populating the account with the user-specific information needed by each service. Source: Sun Microsystems
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system. Source: FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*
Verification	The process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system. Source: FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*
Video Surveillance	An appliance that enables embedded image capture capabilities that allows video images or extracted information to be compressed, stored or transmitted over communication networks or digital data link. Digital video surveillance systems are used for any type of monitoring. Source: Webopedia.com
Virtual Private Network	An Internet-based system for information communication and enterprise interaction. A VPN uses the Internet for network connections between people and information sites. However, it includes stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system. Source: TechDictionary
Vital Records and Databases	Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities. Source: Environmental Protection Agency
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Source: CNSS Inst. 4009, Revised June 2006, National Information Assurance (IA) Glossary
Vulnerability Analysis	A process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use. Source: TechTarget.com

Term	Definition
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system. Source: CNSS Inst. 4009, Revised June 2006, National Information Assurance (IA) Glossary
Web Based Training (WBT)	A generic term for training and/or instruction delivered over the Internet or an intranet using a Web browser. Web-based training includes static methods -- such as streaming audio and video, hyperlinked Web pages, live Web broadcasts, and portals of information -- and interactive methods -- such as bulletin boards, chat rooms, instant messaging, videoconferencing and discussion threads. Source: Webopedia.com
Web Services Security	WS-Security (Web Services Security) is a proposed IT industry standard that addresses security when data is exchanged as part of a Web service. WS-Security is one of a series of specifications from an industry group that includes IBM, Microsoft, and VeriSign. Source: TechTarget.com
Wired and Wireless Network	Refers to any system of transmitters and receivers that sends radio signals over the air, such as a Wi-Fi local network, cellular network or satellite network. Source: Techweb.com