|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **AC313 Chapter 5 Glossary**   |  | | --- | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif |  |  |  | | --- | --- | | **access control** | Control that provides the primary line of defense against most intentional attacks; normally implemented with a layered approach. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **active threat** | Potential intentional attack on the information system. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **application layer** | Data protection that restricts access to specific application programs, such as accounting programs. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **assurance activity** | An activity set conducted as part of security assessment. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **assurance approach** | A general category of assurance methods; organized by ISO/IEC15443 into three general categories that assess the deliverable, the deliverable's development process, and the deliverable's development environment. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **assurance authority** | A person or organization that makes various assurance-related decisions, including the type of assurance to seek and the desired level of assurance. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **assurance class** | A factor that effects evaluation assurance levels. ISO 15408 defines seven assurance classes: configuration management, delivery and operation, development, guidance documents, life cycle support, tests, and vulnerability assessments. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **assurance method** | Recognized specification for assurance activities that yield reproducible assurance results defined as obtaining similar assurance results when different evaluators are working independently of each other. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **availability** | One of the three objectives of information security that involves ensuring that data and information are available when and where they are needed; timeliness is important because information tends to lose value over time | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | ***Baseline Security Manual*** | Security assurance standard that uses a combination of organizational, personnel, infrastructure, and technical security measures to counter a set of well-known vulnerabilities that exist for an "average" organization; emphasizes continuous improvement through monitoring and acting on security problems. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **capability maturity model (CMM)** | Class of process-improvement models defined in terms of the degree of sophistication for a given process; mature processes effect continuous improvement. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **certification registrar** | Body that certifies deliverables against published security standards. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **Certified Information Systems Security Professionals (CISSP)** | Professional organization that provides assurance that an individual possesses an understanding of abroad common body of knowledge relating to information security. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **Common Criteria** | Another name for ISO/IEC 15408; represents a security assurance method and sets uniform standards for evaluating IT security deliverables in three parts: introduction and general model, security  functional requirements, and security assurance requirements. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **composite assurance** | Overall assurance achieved for a given deliverable as a result of using multiple assurance methods. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **confidentiality** | One of three objectives of information security; involves ensuring that data and information are made available only to authorized persons. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **correctness evaluation** | Type of security evaluation that tests only to determine whether the deliverable meets the standards in the defined security target. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **database layer** | Layer of access controls that allows password-based access to application program or database only according to each user's predefined access privileges. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **disaster management and recovery** | Process by which management plans for and responds to possible disasters and substantial business interruptions. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **effectiveness evaluation** | Type of security evaluation that tests to ensure that the deliverable can withstand attacks in the deliverable's operating environment. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **emergency response director** | Individual responsible for emergency preparedness and response; should be in charge of an emergency response center and a supporting emergency response team. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **enterprise risk management (ERM)** | Organizational process that involves weighing various opportunities against related risks and managing the opportunities and risks in away that is consistent with management's objectives and risk preferences. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **evaluation assurance level (EAL)** | One of seven increasing levels of assurance set by the Common Criteria; each represents an increasing level of assurance for a given deliverable. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **Federal Information Processing Standard 140 (FIPS 140)** | U.S. standard published by the National Institute of Standards and Technology (NIST) that defines security requirements for cryptographic security modules in IT products used for sensitive but unclassified purposes. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **gap analysis** | Part of threat and vulnerability analysis that focuses on identifying needed controls not already in place. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **information security assurance (ISA)** | Evidence-based assertion achieved for a target of evaluation by performing assurance activities that satisfy a predefined security target or security protection profile; increases the certainty that a security-related deliverable can withstand specified security threats. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **information security deliverable** | Type of security product defined in the broadest sense to include, for example, information-security-related processes, software and hardware products, systems, services, organizational units, environments, warranties, and even security-related personnel. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **information security management system (ISMS)** | Organizational internal control process that ensures three objectives in relation to data and information within the organization: integrity, confidentiality, and availability. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **integrity** | One of the three objectives of information security; involves accuracy and completeness. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **International Standards Organization (ISO)** | Primary nongovernmental international group that promulgates standards relating to business (and other) processes. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **ISO 27000 family** | Group of ISO standards relating primarily to information security. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **ISO/IEC 13335—management of information and communications technology security (MICTS)** | Standards-based security assurance method that provides a general framework for developing and managing IT security. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **ITSEC/ITSEM—information technology security evaluation criteria** | Forerunner documents to the Common Criteria, widely recognized security assurance methods used throughout Europe. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **layered approach to data protection** | Approach to data security that requires an attacker to penetrate multiple layers of security to obtain access to data. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **loss exposure** | Condition of being subject to loss associated with vulnerabilities in the information system. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **network domain layer** | Level of data security that restricts access to authorized users who typically operate within the local-area network. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **networklayer** | Level of data security that restricts access by means such as passwords, firewalls, and encrypted communications. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **passive threat** | Nonintentional threat against the information system, such as an accident and act of nature. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **penetration testing** | Security assurance method widely used to assess weaknesses in a deliverable by exploiting all possible vulnerabilities; normally conducted after a correctness testing. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **plan-do-check-act (PDCA) methodology** | Systems development methodology often used in the security literature; involves planning (analysis and design), doing(implementation and operations), checking (continuous evaluation), and acting(continuous improvement). | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **primary assurance property (PAP)** | Classification assigned by ISO/IEC 15443 to a given assurance method as defined by its assurance approach and relation to the deployment life cycle. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **process area** | Element of the SSE-CMM® that can be used to define practices that identify the maturity level of a given information security process. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **process control** | Primary benefit of applying capability maturity models that refers to rapid and effective responses to deviations from planned results and in turn to further increases in predictability. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **process effectiveness** | Primary benefit of applying capability maturity models that results in lower costs, shorter development times, higher quality, and higher productivity. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **process predictability** | Primary benefit of applying capability maturity models to produce results that are consistent and according to plans. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **process reference model** | Standardized model or framework for a given process or set of processes; includes SAP R/3, which integrates all major information-related functions in the organization, and SSE-CMM. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **qualitative approach to risk assessment** | Nonmathematical and nonstatistical approach to assessing IS threats, vulnerabilities, and loss exposures; categorizes possible losses according to their severity. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **quantitative approach to risk assessment** | Mathematical and statistical approach to assessing IS threats, vulnerabilities, and loss exposures. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **rating maintenance phase (RAMP)** | Security assurance method that works with TTAP; used to evaluate newer versions of products that already have EAL ratings. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **security assurance model** | Model that specifies how multiple assurance methods work together to yield an overall composite assurance for a deliverable. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **security engineering** | Application of engineering concepts to the development of security processes. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **security protection profile (SPP)** | Protection typically used for procurement; represents the security needs of a given individual or group of individuals. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **security target (ST)** | Set of security specifications and requirements used to evaluate the target of evaluation. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **statement of applicability (SOA)** | End product of the risk assessment process that lists the controls selected and the reasoning for their selection and why other controls were not selected; should be consistent with the ISMS policy developed in the early stages of the PDCA process. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **Systems Security Engineering Capability Maturity Model (SSE-CMM®)** | Same as ISO 21827, which presents a process reference model for systems security engineering. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **target of evaluation (TOE)** | The information security deliverable, the object for which security assurances are made. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **threat** | Impending event that can result in losses to the organization from systems related individuals or events. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **Trust Technology Assessment Program (TTAP)** | Security assurance method that bases evaluations on the ISO/IEC 15408 Common Criteria. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **trusted capability maturity model (TCMM)** | Security assurance method that is a special version of CMM; focuses on security in software development. | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | | | **vulnerability** | Weakness in the information system that exposes it to threats. | |
|  | |  | | --- | | http://highered.mcgraw-hill.com/olcweb/styles/shared/spacer.gif | |