CMMC

(Cybersecurity Maturity Model Certification)

Accreditation Body

Keeping track of the meaning of terms surrounding cybersecurity compliance can be difficult. We get it.

To help with the challenge, we have compiled the following list of terms that we are starting to use internally, refining the definitions as we go along. The definitions are sourced from a variety of organizations, with an attempt to make them easily consumable.

Please send any suggested additions or improvements to: news@cmmcab.org.

Glossary (Draft)

Accreditation – The process of issuing Licenses and Certificates.

Accreditation Body Board of Directors - The board of directors is the governing body of a nonprofit. Individuals who sit on the board are responsible for overseeing the organization's activities. Directors meet periodically to discuss and vote on the affairs of the organization. The board of directors, as a governing body, should focus on the organization's mission, strategy, and goals as defined in the bylaws.

Advisory Councils - Advisory Councils operate at the discretion of, but independently from the board, to inform and advise the board from the perspective of the Advisory Council's membership. The advisory council's leaders participate in the board as a non-voting member.

Affiliates - Business concerns, organizations, or individuals that control each other or that are controlled by a common third party. Control may consist of shared management or ownership; common use of facilities, equipment, and employees; or family interest.

Edward J Kinberg
EJK@StewartLawCS.com
321-541-6845

Assessment - Formal process of assessing the implementation and reliable use of issuer controls using various methods of assessment (e.g., interviews, document reviews, observations) that support the assertion that an issuer is reliably meeting the requirements of a standard. In the context of CMMC, Assessments are performed against the requirements set forth in the CMMC for the OSC's desired CMMC Level. Source: NIST SP 800-79-2 (adapted)

Assessor – A person who has successfully completed the background, training, and examination requirements as outlined by the CMMC-AB and to whom a License has been issued. Assessors are not CMMC-AB employees.

Asset Owner - A person or organizational unit (internal or external to the organization) with primary responsibility for the viability, productivity, security, and resilience of an organizational asset. For example, the accounts payable department is the owner of the vendor database. Source: RMM

Association – The process of linking an Assessor's License Number with the License Number of a C3PAO.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. Source: NIST SP 800-32

Certified 3rd Party Assessment Organization ("C3PAO") – An Entity with which at least two Assessors are Associated and to which a License has been issued.

Certificate – A Record issued to an OSC upon successful completion of an Assessment which evidences the CMMC Level against which the OSC has been successfully assessed.

Certification – The process of receiving a Certificate.

CMMC – The set of standards initially defined by the DoD against which an OSC is to be Assessed.

CMMC Certified Organization – An Organization whose cybersecurity program has received a CMMC Certificate from the CMMC-AB.

Compliance - Verification that the planned cybersecurity of the system is being properly and effectively implemented and operated, usually through the use of assessments/audits. Source: CMM

Edward J Kinberg
EJK@StewartLawCS.com
321-541-6845

Control - The methods, policies, and procedures—manual or automated—used by an organization to safeguard and protect assets, promote efficiency, or adhere to standards. A measure that is modifying risk. (Note: controls include any process, policy, device, practice, or other actions which modify risk.) Source: NISTIR 8053 (adapted)

CUI (Controlled Unclassified Information) - Information that requires safeguarding or dissemination controls pursuant to and consistent with the law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. Source: E.O. 13556 (adapted)

Cybersecurity - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Source: NSPD-54/HSPD-23

Defense Supply Chain ("DSC") - The worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. DSC was substituted for Defense Industrial Base to reflect more specifically the base subject to CMMC assessments.

Digital Signature – An electronic file which is used to authenticate other electronic files and to encrypt files at rest and/or in motion.

Dispute – A formal process managed by the CMMC-AB through which an Assessor and an OSC can seek resolution of a disagreement over the Assessment results.

Dispute Adjudicator – A CMMC-AB employee who is responsible for reviewing and resolving a Dispute.

Educator – CMMC-AB employees who are tasked with educating and testing prospective and current Trainers.

Entity – A legal non-person Organization duly created and maintained under the laws of one or more jurisdiction, including without limitation corporations, limited liability partnerships, limited liability companies, and governmental agencies but excluding unincorporated Organizations such as, without limitation, partnerships.

FCI (Federal Contract Information) - Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments. Source: 48 CFR § 52.204-21

License – A document issued to an Assessor, C3PAO, or Trainer, as appropriate, entitling them to perform their duties with respect to the CMMC-AB as further outlined below.

License Number – A unique identified linked to each Assessor, C3PAO, and Trainer.

Organization - An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements). Source: CMMC

Organization Seeking Certification (OSC) - The Organization that is going through the CMMC assessment process to receive a level of Certification for a given environment. Source: CMMC

Record – A physical document, electronic file, entry in an electronic database, or the like.

Trainer – A person Licensed to provide Training to prospective and current Assessors. The Trainers are not CMMC-AB employees.

Edward J Kinberg
EJK@StewartLawCS.com
321-541-6845