

Definition of Terms

DOE O 414.1C & DOE G 414.1-4 Definitions

Acceptance Testing. The process of exercising or evaluating a system or system component by manual or automated means to ensure that it satisfies the specified requirements and to identify differences between expected and actual results in the operating environment. (ASME NQA-1-2000)

Administrative Controls. The provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of a facility. (10 CFR 830)

Assessment. A review, evaluation, inspection, test, check, surveillance, or audit to determine and document whether items, processes, systems, or services meet specified requirements and perform effectively.

Self Assessment: Performed by individual D/S/C on their own processes

Management Assessments: Reviews of processes performed by personnel external to the D/S/C process owner

Configuration Management. The process of identifying and defining the configuration items in a system (i.e., software and hardware), controlling the release and change of these items throughout the system's life cycle, and recording and reporting the status of configuration items and change requests. (ASME NQA-1-2000)

Consequence. An outcome of an event, hazard, threat, or situation. Source: IEEE Std 1540-2001.

Firmware. The combination of a hardware device and computer instructions and data that reside as read-only software on that device. Notes: (1) This term is sometimes used to refer only to the hardware device or only to the computer instructions or data, but these meanings are deprecated. (2) The confusion surrounding this term has led some to suggest that it be avoided altogether. Source: IEEE Std 610.12-1990.

Functional Configuration Audit. An audit conducted to verify that the development of a configuration item has been completed satisfactorily, that the item has achieved the performance and functional characteristics specified in the functional or allocated configuration identification, and that its operational and support documents are complete and satisfactory. Source: IEEE Std-610.12-1990.

Graded Approach. The process of ensuring that the levels of analyses, documentation, and actions used to comply with requirements are commensurate with— (10 CFR 830)

- (1) the relative importance to safety, safeguards, and security;
- (2) the magnitude of any hazard involved;

- (3) the life-cycle stage of a facility or item;
- (4) the programmatic mission of a facility;
- (5) the particular characteristics of a facility or item;
- (6) the relative importance to hazards; and
- (7) any other relevant factors.

Hazard Controls. Measures to eliminate, limit, or mitigate hazards to workers, the public, or the environment, including— (10 CFR 830)

- (1) physical, design, structural, and engineering features;
- (2) safety structures, systems, and components;
- (3) safety management programs;
- (4) technical safety requirements; and
- (5) other controls necessary to provide adequate protection from hazards.

Item. An all-inclusive term used in place of appurtenance, assembly, component, equipment, material, module, part, structure, product, software, subassembly, subsystem, system, unit, or support systems. (10 CFR 830)

Physical Configuration Audit. An audit conducted to verify that a configuration item, as built, conforms to the technical documentation that defines it. IEEE Std-610.12-1990.

Process. A series of actions that achieves an end result. (10 CFR 830)

Quality. The condition achieved when an item, service, or process meets or exceeds the user's requirements and expectations. (10 CFR 830)

Quality Assurance. All those actions that provide confidence that quality is achieved. (10 CFR 830)

Quality Assurance Program. The overall program or management system established to assign responsibilities and authorities, define policies and requirements, and provide for the performance and assessment of work. (10 CFR 830)

Risk. The likelihood of an event, hazard, threat, or situation occurring and its undesirable consequences; a potential problem. Source: IEEE Std 1540-2001.

Safety. An all-inclusive term used synonymously with environment, safety, and health to encompass protection of the public, the workers, and the environment.

Safety Management Program. A program designed to ensure a facility is operated in a manner that adequately protects workers, the public, and the environment by covering a topic such as quality assurance; maintenance of safety systems; personnel training; conduct of operations; inadvertent criticality protection; emergency preparedness; fire protection; waste management; or radiological protection of workers, the public, and the environment. (10 CFR 830)

Service. Work, such as design, construction, fabrication, decontamination environmental remediation, waste management, laboratory sample analysis, safety software development/validation/testing, inspection, nondestructive examination/testing, environmental qualification, equipment qualification, training, assessment, repair, and installation or the like. (10 CFR 830)

Software. Computer programs, procedures, and associated documentation and data pertaining to the operation of a computer system. (NQA-1-2000)

Suspect/Counterfeit Items (S/CIs). An item is suspect when inspection or testing indicates that it may not conform to established Government or industry-accepted specifications or national consensus standards or whose documentation, appearance, performance, material, or other characteristics may have been misrepresented by the supplier or manufacturer. A counterfeit item is one that has been copied or substituted without legal right or authority or whose material, performance, or characteristics have been misrepresented by the supplier or manufacturer. Items that do not conform to established requirements are not normally considered S/CIs if nonconformity results from one or more of the following conditions (which must be controlled by site procedures as nonconforming items):

- (1) defects resulting from inadequate design or production quality control;
- (2) damage during shipping, handling, or storage;
- (3) improper installation;
- (4) deterioration during service;
- (5) degradation during removal;
- (6) failure resulting from aging or misapplication; or
- (7) other controllable causes.

Verification and Validation. The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements. (IEEE Std-610.12-1990)

Work. A defined task or activity such as research and development; operations; environmental remediation; maintenance and repair; administration; safety software development, validation, testing, and use; inspection; safeguards and security; or data collection and analysis.