		Number: EA CRAD 30-10 Revision: Rev. 0 Effective Date: January 19, 2023
Software Quality Assurance Criteria and Review Approach Document		
Authorization and Approval	DAVID YOUNG Digitally signed by DAVID YOUNG Date: 2023.01.19 16:26:35 -05'00' David A. Young, Deputy Director Office of Environment, Safety and Health Assessments	Digitally signed by Aleem E. Boatright Date: 2023.01.19 16:03:38 -05'00' Aleem E. Boatright, Lead Nuclear Engineer Office of Nuclear Engineering and Safety Basis Assessments

1.0 PURPOSE

The mission of the U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments (EA-30) is to assess the effectiveness of safety and emergency management systems and practices used by line management and contractor organizations and to provide clear, concise, rigorous, and independent evaluation reports of performance in protecting workers, the public, and the environment from the hazards associated with DOE activities.

In addition to the general independent oversight requirements and responsibilities specified in DOE Order 227.1A, *Independent Oversight Program*, this criteria and review approach document (CRAD), in part, fulfills the responsibility assigned to the Office of Enterprise Assessments (EA) in DOE Order (O) 226.1B, *Implementation of Department of Energy Oversight Policy*, to conduct independent oversight and appraisals of high consequence activities. This CRAD specifically provides objectives, criteria, and review approaches to assess the effectiveness of software quality assurance (SQA) programs and processes at DOE sites.

The CRADs are available to DOE line and contractor assessment personnel to aid them in developing effective DOE oversight, contractor self-assessment, and corrective action processes. The current revisions of EA's CRADs are available at https://www.energy.gov/ea/criteria-and-review-approach-documents.

2.0 APPLICABILITY

The following CRAD is approved for use by the Office of Environment, Safety and Health Assessments (EA-30) and sub-tier offices.

3.0 FEEDBACK

Comments and suggestions for improvements on this CRAD can be directed to the Director, Office of Environment, Safety and Health Assessments.

4.0 CRITERIA AND REVIEW APPROACH

This CRAD guides an evaluation of the effectiveness of contractor quality assurance programs for software used at or in support of DOE nuclear facilities in compliance with 10 Code of Federal Regulations (CFR) 830, *Nuclear Safety Management*, subpart A, *Quality Assurance Requirements*, and DOE O 414.1D, *Quality Assurance*, attachments 2 and 4. The CRAD also addresses the adequacy of the Federal review and approval of contractor quality assurance programs for software and adherence to software quality implementing procedures and processes. For safety software, Nuclear Quality Assurance (NQA) -1, *Quality Assurance Requirements for Nuclear Facility Applications*, subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications*, is used as the normative reference. The following objectives, criteria, and lines of inquiry are designed as stand-alone sections to be used in any combination based on the assessment scope. Questions that can be answered with a "yes" or "no" should be followed with an open-ended question to obtain insight and details supporting the one-word response.

OBJECTIVES

SQA.1: The contractor Quality Assurance Program (QAP) adequately implements applicable requirements from 10 CFR 830, *Nuclear Safety Management*, subpart A, *Quality Assurance Requirements*, and DOE O 414.1D, *Quality Assurance*, attachment 2, *Quality Assurance Criteria*, addressing all software, and attachment 4, *Safety Software Quality Assurance Requirements for Nuclear Facilities*, for safety software, and has been reviewed and approved by DOE line management.

Criteria:

1. The contractor maintains a QAP and submits modified QAPs to DOE, if necessary.
2. The approved QAP describes a graded approach, which ensures that the levels of analyses, documentation, and actions used to comply with requirements are commensurate with:
   - The relative importance to safety, safeguards, and security.
   - The magnitude of any hazard involved.
   - The life-cycle stage of the software.
   - The programmatic mission of the facility for which the software is implemented.
   - The particular characteristics of the software.
   - The relative importance to radiological and non-radiological hazards.
   - Any other relevant factors.
3. The DOE-approved contractor QAP includes applicable requirements for all software that are also flowed down into implementing procedures.

4. The contractor applies all requirements applicable to software with the graded approach that is defined and described in the approved QAP.
5. The contractor employs trained and qualified SQA subject matter experts to establish, maintain, and ensure an effective SQA program.
6. The contractor QAP and implementing procedures document the processes and results for identifying safety software as software that:
   - Performs a safety function as part of a structure, system, or component (SSC) and is cited in either a DOE-approved documented safety analysis or an approved hazard analysis per.
   - Is used to classify, design, or analyze nuclear facilities.
   - Performs a hazard control function in support of nuclear facility or radiological safety management programs or technical safety requirements or other software that performs a control function necessary to provide adequate protection from nuclear facility or radiological hazards.
7. The contractor QAP and implementing procedures document the processes and results for assigning grading levels to all software.
8. If software on the Software Central Registry is used, controls for its use are addressed in the QAP and implementing procedures.
9. The contractor ensures implementation of SQA requirements through management and independent assessments.

- How does the contractor ensure an annual review and update (if needed) of the QAP, and timely submission to the DOE approval authority, if necessary?
- Does the approved QAP identify all criteria listed in DOE O 414.1D, attachment 2, that are applicable to software?
- How does the graded approach evaluate the relative importance to safety, safeguards, and security when grading software?
- How does the graded approach evaluate the magnitude of any hazard involved when grading software?
- How does the graded approach evaluate the life-cycle stage of the software being graded?
- How does the graded approach evaluate the programmatic mission of the facility for which the software is being implemented when grading software?
- How does the graded approach evaluate the particular characteristics of the software when it is being graded?
- How does the graded approach evaluate the relative importance of radiological hazards and non-radiological hazards when grading software?
- Has the development of the approved graded approach considered and determined whether there are any other factors relevant to software that affect the grading level?
- Has the contractor assigned an individual(s) responsible for SQA who is adequately trained and qualified?
- How is the flow down of safety software and non-safety software requirements into the site QAP and implementing procedures from 10 CFR 830, subpart A and DOE O 414.1D documented?
- How are the software classification and grading processes described and documented?
- Has all software been evaluated to determine whether it is safety software?
- Has all software been assigned a grading level?
- Does the site use software from the Software Central Registry? If yes, how is documentation of its use addressed in the site QAP and implementing procedures?
- How does the contractor control QAP and implementing procedure updates as changes are made?
- Do management and independent assessments ensure implementation of SQA requirements?

SQA.2: Software selected for review adequately implements site SQA requirements. (10 CFR 830, subpart A and DOE O 414.1D)

Criteria:

1. A software project plan for each software release, developed internally or externally, is defined.
2. The roles and responsibility matrix is provided and gives a clear understanding and agreement on project assignments. It includes individuals or groups responsible for performing specific functions or tasks. After completion, the matrix is then distributed for approval.
3. A software requirements specification is provided and describes the software function and the performance methodology.
4. All software design documentation is written as a report of a software product's design, describing its overall architecture.
5. Software implementation documentation refers to the process of adopting and integrating all software applications into a business workflow.
6. Software validation (test cases, problem reports) determine the correctness of the software with respect to the user's needs and requirements. It is accomplished by verifying each stage of the software development lifecycle. In addition, peer reviews, such as software inspections, are defined and captured in metrics. Audits are developed to assure that all software related action items have been performed. Of those audits, error analysis is performed to prevent, detect, and record errors to ensure high integrity software.
7. Software data collection is gathered, measured, and analyzed as required to research problems, answer questions, evaluate outcomes, and forecast trends and probabilities.
8. User training is documented to enhance performance and adherence to user skill level.
9. Software deliverables are defined by application software related to the specific operating environment. Any enhancements or upgrades are documented. Installation types are identified, and formation documentation is provided.
10. Software documentation of tools and techniques that defines "best practices" and support for the project documentation is provided and reviewed.
11. The software configuration management process is maintained, and results are tracked and controlled as required.
12. The software version is effectively controlled to ensure only the correct version is used. Version control of previous software releases is recorded and documented with related release notes.
13. Successful operations of the software application are planned for, executed, and all activities monitored.
14. Software process assessments are used, based on a process model. The assessment includes the identification and characterization of current practices.
15. Software quality improvement methods are regulated, and corrective and preventative actions are implemented for fixing quality issues to ensure continuous improvement.
16. Archiving software is enabled to move data from production storage to archive storage as needed.

- Do the software plans comply with the QAP and implementing procedures, and have they been documented?
- Is the roles and responsibilities matrix distributed for approval?
- Does the documentation include software requirements?
- Is all software design documentation written in report format, describing overall architecture?
- Does the software implementation documentation refer to the process of adopting and integrating all software into a defined and clear business workflow?
- Does the documentation include software validation such as test cases and/or problem reports?
- Does the documentation include software data collection?

- Is user training documented to enhance performance and adherence to user skill level?
- Are software deliverables defined?
- Does the software deliverable documentation include best practices?
- Is the software configuration management process maintained and results documented?
- Does the installed software reflect the current version and record of previous versions?
- Does the documentation include the planning for and execution of successful operations?
- Is the software process assessment documentation based on a process model?
- Are software quality improvement methods documented and regulated per corrective and preventive actions processes?
- Does the documentation include the data archiving process?
- Does the documentation include a roles and responsibilities matrix?

SQA.3: Software security requirements are integrated within the SQA program or are addressed through established interfaces. (NQA-1, part II, subpart 2.7)

Criteria:

1. Software computer systems and networks are protected from information disclosure, theft of or damage to their hardware, software, or electronic data, using cybersecurity practices.
2. Access credentials, such as access authentication and identification credentials, are implemented.
3. Secure remote access, as a combination of security processes and/or solutions, are designed to prevent unauthorized access to an organization's digital assets and prevent the loss of sensitive data.
4. Clearance level access is required for access to specific classified information. Security clearances are issued for individuals or groups.
5. To block phishing attacks and cybercrime, anti-phishing is enforced.
6. Risk analysis is exercised to eliminate the compromise of a software development project, mitigating the possibility of suffering loss and total risk. (DOE O 414.1D, attachment 4). The risk analysis includes contingency planning and identification of the risk response strategy.
7. Penetration testing is targeted to individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited.

- Are all software computer systems and networks protected using cybersecurity practices?
- Is the practice of access credential authentication implemented?
- Is secure remote access implemented to prevent unauthorized access to sensitive data?
- Is clearance level access required to access classified information?
- Is anti-phishing enforced to block phishing attacks and cybercrime?
- Does the software security include risk analysis and is it documented in contingency planning and a risk response strategy?
- Does the software security implement and document penetration testing?

SQA.4: The Federal program for oversight of SQA is established and effective in ensuring contractor SQA programs satisfy DOE requirements. (DOE O 226.1B)

Criteria:

1. DOE line management reviews contractor QAPs and submitted modifications for approval.
2. DOE line management assigns trained and qualified SQA subject matter experts (SMEs) to oversee the contractor SQA program.
3. SQA SMEs evaluate contractor implementation of SQA requirements.

- How does DOE line management perform and document timely review and approval of contractors' QAP and updates?
- Does DOE line management apply DOE-STD-1172, *Safety Software Quality Assurance Functional Area Qualification Standard*, for the training and qualification of SQA SMEs?
- How do SQA SMEs plan, perform, and document assessments of contractor SQA?
- How does DOE follow up on identified issues and corrective actions?

REVIEW APPROACH

Record Review:
- List of site software applications
- Site QAP review and approval documentation
- Applicable site QAP implementing procedures and records
- DOE and contractor oversight documentation and records
- Software Life Cycle documentation and records for selected software
- Training and qualification documentation and records for selected personnel

Interviews:
- DOE QA Manager
- DOE SQA SMEs
- Software "owners"
- Software users
- Contractor QA Manager
- Contractor SQA independent reviewer

Observations:
- DOE and/or contractor oversight activities
- Configuration Management Review Board meetings
- Meetings associated with safety software determinations
- Meeting associated with software grading activities
- Software field use, input/output