Chair: Vicki Pope

Co-Chair:

Scribe: Marylou Apodaca

**Tuesday, October 29, 2019 – Joint QA Session**

EFCOG’s main purpose is the exchange of information and networking between subject matter experts within each discipline. Therefore, if you volunteer to participate in a task assignment, it is important to really contribute. It benefits the DOE Complex and shouldn’t take too much of your time.

AU-32 Presentation

The SQA SME position should be filled by November 8, 2019

The CGD Handbook is now official

The update to **DOE 414.1-4 SQA Guide** will go back into REVCOM in November. Once the REVCOM review has started, there will be 60 days to comment.

Central Registry Toolbox:

* Implementing corrective actions (this will be one of the assignments for the new SQA SME)
* Working on finalizeing the code priority list (18 sites and 1 federal employee participated in the vote). The list is being resorted to look at how many sites voted for a code, rather than just looking at the total number of votes. This eliminates bias for sites that turned in more votes than other sites. *(See notes under Wednesday’s SQA Sessions for additional discussion.)*

SQA Challenges:

* SQA requirements apply to software beyond Safety Software. However, that requirement is only found in a note in 414.1D. Therefore, the requirement to apply the 10 QA criteria to Non-Safety Software is often missed.
* The definitions of software-related terms in DOE O 414.1D are different from the definitions in DOE O 200.1A (the Information Technology Management Order).
* The emphasis on NQA-1 is not balanced. For instance, there are categories of safety software that are not nuclear or radiological. These types of software, and all other Non-Safety software, can follow a standard other than NQA-1.
* The graded approach is not well defined in O414.1D.
* Not sure how to enforce O414.1D for Non-Safety Software.

AU-32 Priorities for FY20:

* Issuing 414.1-4B Guide on Software Quality Assurance
* Finalizing the Central Registry Corrective Action Plan and begin making those corrections
* Begin the process to update DOE Order 414.1D to 414.1E (major update)
  + AU-32 has one year to develop a vision and approach for the update
  + Will focus on software requirements
  + Requests that SQA practitioners let him (Christian Palay) know what in the current Order works well and what has caused problems, confusions, or other concerns

DOE Order 251 – the definition of “invoked standards”: The new version of 414 will state that if you have a nuclear facility and want to build new or major modification, you must be compliant with NQA-1-2008 with 2009 Addendum or a newer version.

NAP-24A is now officially 401.1

**Tuesday, October 29, 2019 – SQA Sessions**

**Attendees:** *(See signed Fall 2019 Roster in the EFCOG SQA home page – MEETING PROCEDDEINGS – Fall 2019 folder for list)*

**Call in:** (*There were a few technical difficulties, so conference call-in capabilities were abandoned.)*

EFCOG SQA Web Site:

This site is form storing/sharing permanent documents. (Files on the Box site disappear after 6 months if they are not being actively updated. Therefore, that site should only be used for subtask group team collaboration.)

The EFCOG SQA home page has been updated based on the brainstorm suggestions made as part of the SQA team’s Spring meeting agenda.

New features include

* Left side bar:
  + Slide with steps for creating a Box account (with links to the Box site)
  + Quick links to the SQA Documents folder and SQA Meetings folder
* Right side bar:
  + SQA Task Group Charter Statement
  + Placeholder for SQA Task Group Strategic Plan and Guidelines
* Top of page:
  + Contact information for SQA Task Group Leadership
  + Will soon include a picture slide show of photos of our meetings
* Bottom of page:
  + Documents folder:
    - Final products of subtask groups such as white papers, Guidance Documents, etc.
    - Will start adding cover pages to these documents so they can be more easily referenced
  + Meetings Proceedings folder:
    - Subfolders for face-to-face meetings. These contain the meeting agenda, meeting minutes, presentations given, pictures taken during the meeting, copy of the signed roster, etc.
    - Subfolder for WebEx meetings, further subdivided by year, with agendas, minutes, and relevant presentations for each conference call.
  + New folders will be added for older documents extracted from the EFCOG zip file (see Task Group update below), site sharables such as templates and other job aids

Send items for the web site to Vicki Pope, who will then forward them to the proper authority to get posted on the EFCOG SQA page.

Software Gone Wrong

Sid Ailes gave a presentation on three errors discovered by the Atkins company in the ANSYS software and one in the Microshield application (see presentation titled “EFCOG – software errors\_Sid\_10292019.pptx).

1. Atkins was hired to redesign the Hong Kong harbor. INISTATE data for high order beam and pipe elements were giving incorrect results when temperatures were non-zero.
2. Gasket material in tension analysis produced incorrect results when unloading data is not provided. This resulted in a Class 3 Error.
3. When comparing modal solutions with the RSTMAC command of ANSYS, the MAC values may be incorrect.
4. Microshield 3.3 used for geometries with homogeneous materials. MCNP results are either underestimated by factor 0.5 or overestimated by a factor 2 when compared to the Microshield results.

Boeing 737-MAX software issue (see presentation titled “Boeing and FAA certified the suspect 737 MAS flight control system\_fall2019.docx). Boeing claimed that the pilots should have recognized the problem with the stabilizer and should have known what to do without additional training. The failures connected with the MAX airplane involved multiple components – the software performed to its specifications, but was relying on fragile, faulty hardware. The accidents happened in countries in which questioning authority is discouraged (thus pilots relied too heavily on the system to do the right thing). Take away for our group: always keep in mind the software within the system, including interactions with hardware, other software applications, users, and the cultural differences of those users.

Another article on the problems for research studies caused by a code glitch has also been loaded onto the EFCOG SQA 🡪 Meeting Proceedings 🡪 Fall 2019 folder but was not discussed (see file titled “News Article 10- 10-2019 Glitch in Study NMR Code-.pdf”).

Task Group Updates:

* **Zip file (Ashley Toth):**

EFCOG created a massive zip file of old task group documents when it changed to the new web site/format about five years ago. This subtask group has unzipped this file and are reviewing the legacy files to see which ones are relevant to the SQA Group. The unzipped files are on the BOX site. Legacy charters, CGD contributions, investigative reports, and files regarding weapon related software are some of the 300 documents that are being sorted through. Once evaluated, the ones we want to keep will be placed in a folder on the EFCOG SQA page.

* **SCRUM mapping** **(needs a new task leader)**

No progress has been made on this task since the Spring meeting.

* **Cloud hosted software:**

The goal of this task is a guidance paper on steps to assure security if the software tool is hosted on a vendor’s cloud-based server (the user passes data to the application that is on the cloud. – the application then sends the result to the user). These tools are mostly hazard analysis software and design software. Some Cyber Security organizations will not allow their sites to use cloud-based software unless the Cyber team evaluates and approves the vendor setup. Issues include: Safety software vendors insisting that if we use their software it is must be up on the vendor’s server; Automated updates are pushed out and difficult to control. You have no control over change control, configuration management, or companies who may or may not have a standard. Concerns are cyber security and quality assurance. Russel Swannack is leading the effort. If you want to contribute, contact him at russell.swannack@ppnl.gov.

Christian Palay stated that DOE has started using a cloud-based version of SharePoint that was set up by Microsoft for them. He was not sure if DOE has yet to create an official policy on cloud-hosted software but suggests that we make contact with AU-73 (?). The DOE is putting up contracts to vendors to set up cloud-based software.

There still needs to be a way to record the version number and test the software before using the results. Cloud computing needs to be added to QA. DOE and sites are being forced to use cloud based or find something else. GSA is encouraging cloud based. DOE (AU) uses one drive for which they contracted Microsoft to configure the cloud-based instance for them.

* **Toolbox Code Qualification Process Streamlining (Vicki Pope):**

The streamlining process recommendations are almost complete. The task group needs to review and refine the recommendation details from the Spring meeting. Once agreed to, they will be forwarded to Christian Palay (AU-32). It should be completed by the end of November.

* **Strategic Planning (Nathaniel Hein):**

EFCOG promotes excellence in all aspects of the operation, management, and integration of DOE Facilities in a safe, environmentally sound, efficient and cost-effective manner through the ongoing exchange of information on lessons learned.

The SQA Task Group Charter Statement: “The Software QA Task Group (SQATG) serves EFCOG and its members by identifying, analyzing, assessing and recommending methods that support effective implementation of Software Quality Assurance (SQA) requirements and ….” (see the EFCOG SQA page right hand sidebar for the full charter).

If we break down the charter into what is being accomplished, it suggests what the SQATG should be engaged in. Strategic initiatives should be general, high-level areas of focus. For example:

1. Provide standardization DOE complex wide for SQA processes, deliverables, training (for SMEs and SQA in general), etc.
2. Provide leadership to achieve excellence in SQA by right sizing the program by making processes easy to follow, understand, and still remain compliant.
3. Simplify SQA processes and deliverables (such as providing easy to use templates), what goes into the inventory, etc.
4. Possible revisions to document-centric standards (DOE O 414.1D; NQA-1 etc.,) which lead to over emphasis on documentation vs. performance- based assessments.

Quality in general should be the first topic, then software quality to try and change the stigma of SQA, what is the cost of not doing quality (i.e. re-work). Quality is applying an intentional process to ensure a quality outcome. Every piece of software needs some level of quality applied to it-non safety included. Quality implemented on the front end saves cost on the back end. How do we market software quality?

How do we flow down NQA-1 requirements when it was written more towards Civil Engineering? The heart of software is knowing what the requirements are. If you hand the requirements to the developer and they tell you what the development tool is, what’s more important is the “requirements”. NQA-1 is designed heavy towards civil engineering and not to software, these are challenges that we face. That is what gives the impression that NQA-1 is geared only to safety software. LANL, for one, has software (such as chemicals or high explosives) that are just as risk significant but not considered safety software

We need to concentrate on things that streamline SQA standard/policy for DOE. This is what the software community wants. With the DOE Order being Nuclear-centric, we are allowing all other software to go by the wayside. We should be managing “all software”.

SQA needs to develop a close relationship with IT and Cybersecurity to know what they are doing and how.

* **NQA-1 SQA Committee Updates (Sid Ailes):**

Common problem is that the technology and domain knowledge that was in place in 1985 has changed. The lifecycle approach also needs to change. This has led the SQA committee to look at three areas needing improvement:

1. More guidance on software methodology: some users have not understood or taken advantage of defining the software methodology they are really using, therefore, AGILE or SCRUM methodology are not well understood by oversight and site management (and sometime not evenby development teams) or used properly.
2. Guidance is needed on how to apply NQA-1 requirements to non-safety software. It needs to be expanded so that it provides a standard that can as easily be applied to non-safety software.
3. More guidance is needed on how to apply NQA-1 to Agile development and methodologies. Kary Cook is working on how to do that.

* **DOE G 414.1-4 - Software Guide Revision (Christian Palay):**

The guide revision, which is expanded to include non-safety software, will be going back into REVCOM. Not much has changed in this revision from the one sent out in 2013-2014. Rehashing old arguments / comments will hold up the process. REVCOM is a 60-day review. Then comments will be addressed and hopefully, DOE will be able to reach concurrence with the sites. To be a reviewer you need to either contact your site’s REVCOM designee or sign up on the DOE REVCOM site (<https://directives.doe.gov/revcom>).

How do we get buy in from the non-safety software users to do SQA on their software? Other software costs a lot of money for new software new versions sometimes don’t bring over the existing data and the issues are not tracked for cost. Stakeholder confidence is a risk, apply appropriate rigor. Changing culture for non-safety software is a problem. Cost/Risk analysis is expensive. Money is also being sent on help desks, etc. Cost should be an issue or category considered in the graded approach.

Update to DOE O 414.1D (i.e., 414.1E):

AU-30 has given AU-32 (Christian Palay) one year to gather justification to update DOE Order 414.1D. This would be a major change (e.g., move to 414.1**E**). The EFCOG SQA Group could weigh in on some of these during our monthly conference calls or at the Spring 2020 meeting. Some of the issues/problems with .1D include:

* How to define “software”? DOE Order 200.1A has a definition of software that is different from that in 414.1D.
* How do we integrate with other orders that have software implications? For instance, O 200.1A requires IT to have an inventory of “all” software. Cyber Security adherers to Order 205.1C. Need to work with IT, Cyber Security. What are all the orders and other documents (policies, guides, standards) that affect software (all software)?
* The requirement to apply the Quality Criteria to software is found in a footnote. How to we integrate it (software) more in the actual Order and make it more of a focus?
* The current requirements are geared more toward hardware. How do they need to be changed or expanded to be more relevant/applicable to software?
* Order 414 requires but does not define a graded approach. Should it? If so, what should the graded approach be? What categories should be included/considered?
* Is NQA-1 the right standard for software? ASME has told DOE that they will not develop a separate standard for non-safety software. If asked to expand NQA-1, the ASME board will find someone else to do it. NQA-1 is going to work on being more process based. There is a movement that if a site or facility is less than HAZCAT 3, they don’t need to do anything SQA – at least not be required to do specific SQA. Other standards, such as ISO-9001 and the IEEE standards could apply, but all of them have their drawbacks. Christian is willing to consider alternatives to NQA-1, we just need to make the case for something better. There is so much diversity in the sites so that needs to be kept in mind to meet the needs of the sites. There’s NQA-1 for software and how do you implement, IEEE Standards are more known to industry and that’s the standard most sites use. Some feel that DOE needs to dictate a standard so that all sites are standardized. Standard should apply to both safety and non-safety software.

Miscellaneous Discussion Points:

* Start using the toolbox criteria for SQA assessments across our sites so that all sites are doing the same thing.
* SQA has a bad reputation amongst most developers and managers. How can we improve our “image”?
  + SQA resources are not readily available-we need to educate our engineering staff better on the why of software quality.
  + If the SQA Program is too complicated, no one will follow it. We have to make or programs and following them the simple solution.
  + SQA should flow from the general QA program.
  + We need to re-educate people on what QA is and what it is not.
* A listing of all safety software used across the Complex might be a future request (target common applications for the Central Registry Toolbox).
* Should enterprise software (e.g., Microsoft Word) be included in the Software Inventories?

**Wednesday, October 30, 2019**

Pain points:

* What do you include in the inventory? Excel, CAD etc.
* What do you exempt? IF something is exempted, how do you record that and what do you still require, if anything?
* Define quality affecting software?

The DOE Software Guide:

Not many changes since the 2014 version. Will hopefully go into REVCOM again next week. REVCOM will last approximately 60 days. There is a backlog of policies and guides that need to get through the review boards.

Find out who at your site gets notified of REVCOM reviews and make sure they know/understand to forward all software-related reviews to you. Or, you can go to <https://www.directives.doe.gov/revcom> and sign up for notifications.

If at all possible, look for solutions to issues so as to not hold it up with too many major comments. Talk to your field office representatives and request that the Guide be approved.

Cyber Security Presentation (Tony Hickey, CNS):

Cyber Security Requirements vs SQA – Antonio Hickey, CNS Cyber Security Authorizations Manager

The Cyber Security program must follow DOE O 205.1C. This order does not mention Quality Assurance. The SQA program must follow DOE O 414.1D, which doesn’t mention cyber security. The IT program follows DOE O 200.1A, which doesn’t mention Quality Assurance or cyber security. This leads to very stove-piped implementation of the three programs.

DOE O 205.1C:

* Lays out NPO Authorizing official, cyber approval to operate guidelines/requirements
* Risk based utilizing risk management framework (RMF)
* Requirements flowed down to tactical CNS Guidance
* Risks captured in information system plan (SSP)

DOE O 414:

* Does not mention cyber security program guidance
* Defines Quality levels
* Applies graded approach, but does not define it
* Requirements flowed down in CNS’s Technical Evaluation Guidance document
  + Defines cybersecurity involvement

Cyber Approval:

* Information systems must have an approved information system security plan (ISSP).
* ISSP security controls are defined by the National Institute of Standards and Technology (NIST) (Unclassified) or the Committee on National Security Systems Instruction (CNSSI) 1253 (Classified).
* Cyber Evaluation of Changes to ISSP begins with a Cyber Security Impact Analysis (CSIA). These can be as quick as 1-2 days. Bigger systems or systems with more potential vulnerabilities will take longer.
* CSIA documents hardware/software deployment and describe their security significant features.

The Cyber program look at all hardware and software to evaluate them for vulnerabilities, risk assessment, and threat models. The Cyber Review Board analyzes high-level threat and determines what steps are necessary to protect the site from those threats. This threat modeling is above and beyond the typical SQA risks. The cyber program documents (approvals, threat models, risk assessments, etc.) are good for three years or until deployment changes.

The Cyber Security Program doesn’t actually like in-house developed software because it must rely on the internal staff to do vulnerability evaluations, which are rarely done.

What about Cloud Application (SaaS)?

* Cyber requirements are the same, with a few exceptions.
* Cloud solutions will have an ISSP.
* Cloud solutions providers must have FedRAMP Certifications. Under FedRAMP. Cloud applications will have an Approval to Operate (ATO) from the Federal govt.
* Security Controls within the Cloud will be inherited.
* Monthly continuous monitoring.
* Cyber does have some input into procurements approval.
* There must be some level of trust between the site and the vendor of Cloud-hosted software. Therefore, the Cyber group is not concerned with update to software that they have previously approved. They are more concerned with updates to the client-side machines.

For all Cyber concerns/evaluations, they look at *Integrity, Confidentiality,* and *Availability* to determine the risk or vulnerability level.

Integrating Cyber Security and Software Quality Assurance at ORNL:

(presentation by Kevin Shaw – see presentation slides on the EFCOG SQA site)

Slide 11 SQA / Cyber Requirements Roadmap represents the flow of software/cyber-related requirements from:

* Federal standards, orders, laws, and policies (shown in primarily white boxes) to
* ORNL’s software guidance document sections/requirements (blue and yellow boxes), which contains both SQA and cyber requirements. The SQA Guidance document spells out the *process* [what needs to be done]. These point to
* The Software Engineering Program’s Guide documents (green boxes), which are umbrella governing documents and include the relevant requirements from cyber, SQA, IT, and self-imposed. These point to
* Work procedure/instruction documents (orange boxes) gives step-by-step instructions with links back to the requirements and governing document sections and spells out *how* it is done.

All steps are followed for both safety and non-safety software. The effort is also integrated with the procurement process. They have monthly meetings attended by representatives from SQA, Cyber, IT, and Procurement.

Central Registry Toolbox Qualification Criteria (60 page document)

Includes questions for the 10 DOE O 414.1D work activities plus sections for modeling and Quality Assurance Program Implementation. Responses to the Criteria review, which took place over the summer, were reasonable. These criteria are meant more to evaluate the vendor and not the software.

Deb Sparkman is currently qualifying SharePoint, so modification of the Central Registry is on hold right now. DOE has a restart plan for once the new SQA SME is hired. The main point of the Central Registry is model validation.

The results of the Toolbox Code vote conducted by the SQA group during the Spring 2019 meeting were reviewed. Since a few sites had multiple voters and other sites had only one or two, they analyzed each tool for the number of sites that voted for it. This caused the top ten to fall out differently. The new Top Ten list is as follows:

1. MCNP (11 sites voted for this application)
2. HotSpot (11 sites)
3. SCALE (8 sites)
4. ALOHA (8 sites)
5. EPICode (7 sites)
6. ETAP (6 sites)
7. MACCS (6 sites)
8. RADCALC (6 sites)
9. SAP2000 (5 sites)
10. ANSYS Fluent (5 sites)

AU-32 will be soliciting input from safety basis and fire protection groups to gather codes they use.

Sites are duplicating effort by each qualifying these applications on their own, but there is not a good way to share our assessments. Software downloaded from the Toolbox still has to follow an SQA process, but you don’t have to do vendor sourcing, assessment of the vendor’s program, or model validation.

If a site puts a vendor on the MASL, software should be evaluated in the same manner using the Toolbox criteria. These assessments could be multi-site evaluations. If the limitations can be worked through it could be cost effective. Benefits would include collaboration to implement evaluation, knowledge base increasing, qualifying EFCOG SQA members to assist in conducting the Toolbox Qualification process, build expertise among members, shared resources.

Some ways to assess software: Assessee fills out the column that says what document/objective evidence meets the criteria. Checklist of the requirements from 414/NQA-1, may also look at software being used and how it’s used.

One bottleneck is that Toolbox qualifications must be led by a federal employee who has been qualified to DOE Std 1172. These would mean that at most, only two Toolbox qualifications could be done a year.

Are DOE SQA Requirements Too Document Heavy?

Difference between criterion-based audits vs process or performance-based audits.

Legitimize tools (e.g., Requirements management tools, defect tracking tools, etc.) and standards/procedures for how to use those tools for your SQA documents, records, and traceability.

Using AGILE methodology, use tools such as GIT (has the requirements, tool, change request and associated tools). What GIT does not have is a tool to print all requirements. There are different tools available-it is not clearly defined if the tool is a record repository. It would be more efficient than a document repository. The point is that you aren’t producing documents per se, but (electronic) records that are traceable. The only problem with AGILE you have to have tools to capture the information or you’ll lose it or end up doing reverse engineering.

Governing documents need to be well written. Document how to use the tool, all the information is contained, and standards are updated and made live. Some of the problems may be how do you know if the documentation was reviewed and approved? Should have doc control (external) – someone has to be responsible for release etc. Roles and responsibilities need to be well defined. Corrective actions/work arounds are another area that needs to be addressed.

The SQAP has to have all of the details even if you are using electronic tools for requirements, design, and test, you could make these requirements, design, test into a pdf. This is standard industry practice. The tools can be tailored to process. Data is stored “forever”. There’s backup, recovery and storage on site.

This is something that would be useful in the future. We are decades behind industry and should consider benchmarking such industries as Medical or Banking who are already doing this. We could piggyback off what they already have in place. This would be a good topic for a future WebEx.

Task Brainstorming Session

Start with the end in mind-what do we want to accomplish? What tasks do we want to work on?

Current Task Groups:

* Toolbox Qualification Process Streamlining
  + Status: Almost done. Need to finish reviewing detailed recommendations. Hope to complete by end of calendar 2019.
  + **Vicki Pope (LLNL) – leader**
  + Cliff Glantz (PNNL)
  + Roger Lanning (Hanford)
  + Keith Morrell (NNSS)
  + Carol Olijar (ANL)
  + Russell Swannack (PNNL)
  + Dave Thoman (AECOM)
  + Ashley Toth (Hanford)
* MASL SQA Checklists
  + Status: Partially complete. Suggest doing a crosswalk with the Toolbox Criteria or use those for the checklist
  + **Kary Cook (PNNL) – leader**
  + Yevonne Deaton (DOE EM)
  + Kevin Shaw (ORNL)
  + Roger Ward (CNS/Pantex)
* SQA Zip File
  + Status: Almost done. Estimated completion is end of November 2019
  + **Ashley Toth (Hanford) – leader**
  + Kary Cook (PNNL)
  + Dave Thoman (AECOM)
* SQA Task Group Strategic Plan
  + Status: Draft guidance; should be ready to present final at Spring 2020 meeting
  + **Nathaniel Hein (LANL) – leader**
  + Teri Vincent (Y-12)
  + Marylou Apodaca (SNL)
  + Greg Smith (LANL)
  + James Hylko (Paducah)
* Work Activities to SCRUM Mapping
  + Status: Preliminary work done during Spring 2019 meeting
  + **Stella McKirdy (INL) – New leader**
  + Sid Ailes (Atkins)
  + Kary Cook (PNNL)
* Cloud-Hosted Software
  + Status: Have gathered some information. Possible completion by Fall 2020 meeting
  + **Russell Swannack (PNNL) – leader**
  + **NEEDS TEAM MEMBERS**
* **NEW TASK: How to manage configurable devices**
  + (white paper or guide). Draft up some type of process/procedure document. Present results/draft at the next spring or fall EFCOG meeting.
  + Includes configurable devices and virtual machines/networks
  + How do you define and grade?
  + When do you integrate cyber security?
  + How and when do you apply SQA?
  + Where are we vulnerable?
  + How do you define change management?
  + How are you capturing the information?
  + What do requirements say? What should the requirements be?
  + Should this be clarified in DOE O 414.1E?
  + Include/use the Firmware White Paper
    - **Veronica Camarillo-Morris (LANL) -- leader**
    - Lance Abbott (SRS)
    - Cristy Renner (PORTS)
* **NEW TASK: Matrix of Orders and Policies Effecting Software**
  + What are the policies, procedures, orders, standards, etc. that have software elements that effect how we “software” within the DOE?
  + Create a matrix of the document and what it says about software
    - **Gary Heidel (ETTP) – leader**
    - Clyde Armstrong (Tru Project)
    - Vicki Pope (LLNL)
* **SPRING MEETING TOPICS:**
  + **Training**
    - How are you doing training at your site?
    - How do we train SMEs whose main job is not software development (best practices etc.)?
    - Basic Awareness
    - SQA Nomenclature
    - SQA SME training for organizations
    - Owner responsibilities
    - Supplier Audits
    - training for engineers who develop software
    - National Training Center (NTC) has a training database
    - Cristy Renner (PORTS) will do a synopsis of the Linda Westfall class at the Spring meeting.
  + Audit Findings
    - Share findings we found disagreeable and discuss
  + SQA/QA Rebranding
    - People dislike, distrust, or misunderstand what SQA and QA really is. Brainstorm ways to re educate people and give SQA/QA a better image
* **DOE O 414.1E** **Update**
  + Christian Palay needs to justify the need to change the order.
  + Start addressing the following task list during future WebEx meetings:
    - Define “software”
    - Better define “graded approach”
    - Better define exemptions and scope of Inventories – both safety and non-safety. Give examples/list exemptions (Christian does not want to put exemptions in the order. This would be more for site use.)
    - How to better include non-safety software (currently in a note)
    - Document the matrix: Put it together and send to the group at some point in the future. (see New Task above)
    - How to “legitimize” tool use for records (e.g., Jira, Git, Confluence, etc.)
    - Clarify, identify, and control of items (software)
    - Take the word “nuclear” out
    - Base graded approach on intended use and/or impact?
    - Alternate standard? What is the industry standard? What does apple or google use? This could be a spring topic. Maybe pulse industry-Microsoft, Apple or others.
    - Explore the history of the Order – how it evolved, why certain directions/decisions were chosen (e.g., why NQA-1, etc.)
    - What do we LIKE in the Order?
* Next Teleconference Call: January 15th, 2020; 1:00 pm PST

**October 31, 2019**

CNS Configuration Management Plan Template and Database Presentation (Teri Vincent, CNS)

Teri Vincent shared the CNS Configuration Management Plan template (Word document) with the group. The information from this template is entered into SMAN, a SAP database, that captures and stores the information captured on the form, among other application artifacts. (See the template on the EFCOG SQA page under the Meeting Proceedings 🡪 2019 Fall Meeting folder. The file is titled “CNS\_Configuration Management Plan\_10.24.19\_DCRO.pdf”.)

The form already has many “standard” information filled in, but modifiable, such as Roles and Responsibilities. This saves users time and effort while providing guidance as to the type and level of detailed information being requested. The template could be easily adapted for use at any site, although the underlying database would need to be developed unless your site also has SMAN.

The information also has the ability to create parent/child associations, for instance:

Parent: Large system XXX

Child: Module A of Larch system XXX

Parent: All commercial High-Risk applications

Child: individual applications within that category

This allows umbrella information and processes to be kept at the “parent” level (e.g., an umbrella SQAP and SCMP, Test Plan, etc.), while individual differences and related documents are kept at the “child” level (e.g., process difference, test cases/results, configuration items for that app, versions, etc.).

Application documents and all changes are managed through their SMAN system, including change control and approvals. The system also tracks and manages errors. For instance, if a system or application goes down, the SMAN database alerts all known users of the application to the difficulty and how to proceed.

Recently, the system began tracking non-conformances to procedures as well as changes to code.

Legacy codes have to have high-level artifacts normally associated with an in-house developed project such as requirements (perhaps in the form of features needed), tests, and a configuration management plan via the template.

The approval stream for new applications and updates to existing applications includes the Cyber Security group.

This database currently includes desktop tools like operating systems, Word, Adobe, etc. These types of commonly used apps are classified in the system as a “tool” , which greys out all fields except titles and versions, meaning they are exempt from the rest of the SQA program. Patches of these types of “tools” are cataloged and managed by the system, if they are properly entered. The Information Technology (IT) and Cyber Security groups are the biggest offenders for not putting all of their applications into the system.

SRNL stated that all their safety software is on a network that does not ever get auto patches/updated to operating systems and support tools. They must be notified of upcoming changes so that a test environment can be created to test how the change will affect the safety applications. This gives the software owners and system administrators a change to correct/update the safety apps prior to the system patches.

Gary Heidel has created a requirement traceability spreadsheet that he will share with the group.

Many sites stated that they do not allow any of their employees to download software or updates – they must all go through the IT group. IT reviews, approves, and “pushes” the downloads/updates to the users or, adds applications to a site-owned download manager application from which individuals can download commonly used applications.

Other sites stated that their SQA Office is integrated with Procurement such that all software-related procurements must be reviewed and approved by the SQA Office prior to purchase/acquisition.

CNS has NO exemptions from software being entered into their SMAN software inventory. Depending on the risk grading as part of the entry process, SQA requirements range from formal documents and SQA practices to almost nothing in the way of QA/SQA (very low-risk applications).

* Next Teleconference Call: January 15th, 2020; 1:00 pm PST