# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Document Version | Author | Date | Description |
| 1.0 | Nate Lee | 2020-03-31 | Initial draft. |
| 1.1 | William Riviere | 2020-05-19 | Updated DRP Rating Scale Table, email template, and review times. |
| 1.2 | Nate Lee | 2020-06-02 | Minor updates to Workflow figure, Rating Scale table, and email template text. |
| 1.3 | Nate Lee | 2020-09-24 | Updated Rating Scale table and email template text. |
| 1.4 | Nate Lee | 2020-09-25 | Updated email template text. |

# Overview

This process details the activities the members of the Adaptive Capabilities Testing (ACT) Deliverable Review Panel (DRP) must perform to receive and review the various ACT contract deliverables. The DRP reviews each contract deliverable to determine whether or not it should be accepted or rejected by the contract Government Task Lead (GTL). This recommendation from the DRP is generated by rating the ***content*** and ***quality*** of each deliverable using a 5-point scale, with the overall rating of the deliverable being the lowest of those two ratings, and the recommendation coming from the overall rating.

Figure 1: ACT Assessment Workflow shows where the DRP is involved in the typical ACT Assessment Workflow:



Figure 1: ACT Assessment Workflow

The DRP typically reviews six (6) ***types*** of artifacts, for a ***total of eleven (11)*** artifacts per typical ACT assessment:

* **Security Assessment Plan (SAP)**: Draft and Final
* **Risk Assessment Plan (RAP)**: Draft and Final
* **Security Assessment Report (SAR)**: Draft and Final
* **Risk Assessment Report (RAR)**: Draft and Final
* **Findings File**: Draft and Final
* **Risks File**: Draft and Final
* **Final Package**: Final

# DRP Membership

The DRP membership will comprise experts identified by the ACT contract GTL who are qualified to review ACT contract deliverables and determine whether or not they meet all applicable contractual, content, and quality requirements.

## DRP Roles and Responsibilities

There are two (2) roles that can be filled by DRP members:

* DRP Chair:
  + One (1) person fills this role, unless multiple DRP Chairs are named by the GTL.
  + Determines which DRP Reviewers will review which deliverables.
  + Consolidates feedback from the various DRP Reviewers.
  + Reviews and ensures the consistency, quality, and content of the DRP’s feedback.
  + Tracks the ratings for each reviewed deliverable in the DRP Review Tracking Sheet.
  + Acts as the single “voice” of the DRP by submitting all DRP feedback to the ACT Assessment Team.
* DRP Reviewer:
  + Multiple people fill this role.
  + Reviews, analyzes, and documents (in the form of either Tracked-Changes or Comments) feedback for the author of each reviewed deliverable.
  + Separately rates the document’s Content and Quality.
  + Documents the Content and Quality ratings, along with the Overall Rating, as a comment on the title page/first page of the reviewed deliverable.
  + Provides the reviewed and commented deliverable to the DRP Chair for review and submission to the ACT Assessment Team.

# Deliverable Review Process Description

The DRP review process for each deliverable is, in many ways, an inherently ***qualitative*** process that the DRP process ***quantifies*** at the end.

## DRP Reviewer Process Description

The DRP Reviewers first review and analyze the content and quality of every part of the deliverable, considering questions and concerns such as:

* What is the overall intent of this deliverable, and what is the specific intent of the specific section of the deliverable that I am reviewing? Are these intents achieved by the content provided (content), and by the way (quality) that they are presented?
* Who are the intended readers, and who are the likely readers, of this deliverable (and the currently reviewed section of the deliverable)? Are those readers likely to understand content as presented, and are they likely to walk away believing that their questions were satisfactorily answered or that their concerns were satisfactorily addressed?
* “*Hard writing makes easy reading*”: did the author put in sufficient effort to make reading and understanding the deliverable appropriately easy, or is the author taking short-cuts that make the document unnecessarily hard to understand, open to confusion or misinterpretation, etc.?
* Does the deliverable “stand on its own” – is special or current knowledge about the system or its context required in order to make sense of the content, or does the deliverable sufficiently lay out necessary context or special information so that someone new to the system will be able to understand everything several years from now?
* Does the deliverable seem “professional” and does it “give a good impression” and “inspire confidence”? If not, why not?
* Is this a deliverable that you (the DRP Reviewer) would be content to personally present to the CISO[[1]](#footnote-1), CIO[[2]](#footnote-2), or authorizing authorities for review and to answer their follow-up questions?

While reviewing the deliverable, the DRP Reviewer documents (in the form of Tracked-Changes or Comments) any significant errors or problems identified with the content or quality, making comments as appropriate to clearly communicate to the DRP Chair, deliverable author, and the ACT Assessment Team what questions or problems the DRP Reviewer encountered while reviewing the deliverable. Every comment should be prefixed with one of the following labels:

* “**Problem:**” The DRP Reviewer has identified a noteworthy issue with the deliverable that ***must be addressed*** prior to submission of the deliverable to the system team.
* “**Potential** **Problem:**” The DRP Reviewer is unsure whether or not there is a problem – the author must ***consider*** the comment and ***take appropriate action*** (including potentially communicating directly with the DRP Reviewer) prior to submission of the deliverable to the system team.
* “**Suggestion:**” The DRP Reviewer has identified an area for improvement that ***may*** be addressed prior to submission of the deliverable to the system team.
* “**Observation:**” The DRP Reviewer wishes to communicate something to the author that does not require a change to the deliverable.

The DRP Reviewer must commit a reasonable amount of time to reviewing the deliverable; the amount of time is variable, and at the discretion of the DRP Reviewer. Based on DRP experience to-date, the following are good “rules of thumb” for planning review times for “good” deliverables:

* **Draft SAP**: 60 minutes
* **Draft RAP**: 45 minutes
* **Final SAP**: 15 minutes
* **Final RAP**: 15 minutes
* **Draft SAR**: 60 minutes
* **Draft RAR**: 45 minutes
* **Final SAR**: 15 minutes
* **Final RAR**: 15 minutes
* **Draft Findings File**: 15 minutes
* **Draft Risks File**: 15 minutes
* **Final CAAT**: 5 minutes
* **Final Package**: 15 minutes

If during the review process it becomes clear that the review will require significantly longer than these general timeframes, it likely indicates that there is a major problem with the deliverable, and the DRP Reviewer should consider ending the review early and rating the document based on the review performed so-far. In such a case, the fact that so many or such large problems are slowing the review is likely reason to end the review early and reject the deliverable.

## DRP Reviewer Reporting Process Description

After sufficiently reviewing the deliverable, the DRP Reviewer uses the table below to determine which rating to give the deliverable for ***content*** and for ***quality***. The choosing of these ratings is qualitative and is based on the qualitative criteria listed in the table. These choices result in quantitative ratings based on qualitative criteria.

Table 1: DRP Rating Scale

| **DRP Rating Scale** | | **5** | **4** | **3** | **2** | **1** |
| --- | --- | --- | --- | --- | --- | --- |
| **Overall** | **General Description** | A great example. | Fine - "ticks all the boxes" but could be better. | Requires more work and polish. | Seems like a rough draft. | Questions competence of authors. |
| **General Sentiment** | "We're proud of this document. We have confidence in this document." | "We're 'OK' with this document (but might require minor changes before acceptance)." | "This wasn't quite ready for submission." | "We definitely should not have seen this version of the document." | "This document is embarrassing." |
| **Acceptance Description** | Acceptable without hesitation. | Acceptable (possibly with changes required). | Unacceptable, but close. | Unacceptable. | Completely unacceptable. |
| **GTL-Specified Acceptance Decision** | "Acceptable" | "Acceptable" | “Unacceptable” | "Unacceptable" | "Unacceptable" |
| **Content**  *(Typical Potential Descriptors)* | | - Demonstrates mastery of system, environment, requirements, findings, and risks - both at system-level and Enterprise-level.  - Explains things clearly and adequately.  - Tells coherent and compelling "story".  - Test and evaluation activities are comprehensive and fully appropriate. | - Demonstrates good understanding of system, etc., but there may be a few holes.  - Story told well but could be improved.  - Test and evaluation activities are adequate and appropriate but might not provide full coverage. | - Demonstrates only shallow understanding of system, environment, risks, etc. and their effects on the Enterprise.  - Might be confusing or incomplete but still paints a reasonably detailed picture.  - Test and evaluation activities not quite adequate or appropriate. | - Important details missing or wrong, chunks missing from the "story", confusing or misleading, major consistency issues.  - Major deficiencies in test and evaluation activities. | - Misunderstand system or requirements.  - No understanding of effect on Enterprise.  - Poor explanations. Confusing or misleading.  - Incomplete details or context.  - Little-to-no appropriate testing or evaluation performed. |
| **Quality**  *(Typical Potential Descriptors)* | | - Contains very few technical, consistency, grammatical, formatting, (etc.) errors.  - Shows great care and attention to detail.  - Looks and feels polished and professional. | Reasonable tech-edit/QA seems to have been done, but sometimes "missed the point". | Significant occurrences of QA failure suggest that QA was incomplete. | Rudimentary QA seems to have been done - many errors still present. | Clearly no meaningful tech-edit or quality control - numerous/egregious errors in grammar, consistency, technical details, etc. |

The DRP Reviewer documents these ratings, along with the Overall Rating (which is the lowest of the content and quality ratings), in an email, and then sends the marked-up deliverable in that email to the DRP Chair. The following email template should be used; replace the yellow-highlighted text with actual text, and leave the red-highlighted text highlighted and unedited:

**Subject**: DRP Review: SYSTEMNAME DELIVERABLE(S)

**Body**:

DRP Chair,

The following **SYSTEMNAME** deliverables have been reviewed and rated using the DRP Rating Scale provided in the current version of the Deliverable Review Process document. **Note that these deliverables require extra scrutiny from you – see the specific feedback in the email text below.**

* This version of the DELIVERABLE received an **overall rating of X** (out of 5), scoring **X for Content** and **X for Quality**.
* This version of the DELIVERABLE received an **overall rating of X** (out of 5), scoring **X for Content** and **X for Quality**.

The DRP review email text to send out is provided, and the DRP review comments are attached to this email. ***Be sure to choose the appropriate acceptance status(es) in the email text below prior to sending.***The authors of these deliverables are: **AUTHORNAME**.

=====

ACT Assessment Team,

The Deliverable Review Panel (DRP) review of the following **SYSTEMNAME**deliverables is completeand feedback is attached.

* This version of the DELIVERABLE is **acceptable/unacceptable**.
* This version of the DELIVERABLE is **acceptable/unacceptable**.

The following non-comprehensive feedback is called out here for emphasis:

* FEEDBACK

Please let us know if you have any questions or concerns.

## DRP Chair Process Description

The DRP Chair is responsible for ensuring that deliverables are reviewed by appropriate DRP Reviewers. The DRP Chair assigns deliverables to DRP Reviewers as she deems appropriate; for example, the DRP Chair might determine that a DRP Reviewer will always review deliverables that come from a system for which that person is also the Cyber Risk Advisor (CRA).

The DRP Reviewers submit all of their reviewed and marked-up deliverables to the DRP Chair. The DRP Chair then performs a secondary “sanity check” of the reviewed deliverable to ensure the consistency, quality, and content of the DRP Reviewer’s feedback. The DRP Chair makes any changes to the DRP Reviewer’s feedback and/or ratings that she deems appropriate, communicating with the DRP Reviewer as appropriate to clarify questions or concerns and to explain important changes to their feedback.

The DRP Chair records the final content, quality, and overall ratings in the DRP Review Tracker. The DRP Chair then submits the finalized feedback and ratings to the ACT Assessment Team. The email template included in the email from the DRP Reviewer should be used (and customized as appropriate).

1. CISO: Chief Information Security Officer [↑](#footnote-ref-1)
2. CIO: Chief Information Officer [↑](#footnote-ref-2)