

APPENDIX E – JITC RISK ASSESSMENT METHODOLOGY

INTRODUCTION

The fundamental risk assessment guidance for the Department of Defense (DoD) is the "Risk Management Guide for DoD Acquisition." Although the principles explained in the guide are not mandatory, they are recommended and applicable to DoD Information Technology Standards Registry (DISR) and non-DISR standards. Testers must prioritize standards conformance testing by calculating the risk for the Technical View (TV)-1 standards implementations in the system under test. The following document provides a framework for testers to perform a correct and organized analysis of risk factors.

By organizing the risk analysis, potential issues may be eliminated from consideration due to low mission impact and/or low probability of occurrence (likelihood of failure). Test scope may be reduced through the elimination of information exchanges that exhibit low risk (the product of low impact and/or low probability of occurrence of each potential issue). The secondary effect of this organized analysis will be to maximize accuracy and confidence in the risk assessment. Both will result in a more defensible scope of standards conformance testing.

BACKGROUND

The Joint Interoperability Test Command (JITC) determined that, across the Command, there was a lack of consistency in the determining risk level for standards. In response to this issue, the JITC Standards Research (JSR) Team was formed. The JSR Team collects test methodologies, recommended test tools, known issues, and guidance from test facilities and experts across the Command. The JSR Team maintains the data through regular interviews with Subject Matter Experts (SMEs) and regular updates from the DISR. The JSR Team developed the JITC Risk Assessment Database (J-RAD) to provide Information Technology (IT) standards testing information to program managers and JITC personnel for the purpose of supporting interoperability testing and certification efforts.

The JSR Team, along with the J-RAD, provides a one-stop resource for IT standards information. The J-RAD contains selected data fields from the DISR, including maturity rating, abstract description, applicability information, and other details. The JSR Team also researches other standards that appear in system documentation, but are not listed in DISR, and accumulates that information in J-RAD. The J-RAD includes information about available test tools, methodologies, and test facilities/organizations, as well as links to Web sites of organizations concerned with the development, approval, and implementation of IT standards. All database records on test tools are tagged with the organization that developed the tool, a description of what

the tool does, whether JITC uses the tool, and other useful information. All database records on test facilities/organizations include a description of capabilities and contact information.

Self-Service J-RAD. Testers can use J-RAD on a self-service basis via Defense Information Systems Agency network methods. The J-RAD generates a high-level view of standards listed in their TV-1 and provides a summary of known uses of each standard and the accumulated known issues that represent the potential risks to the system. While this is a good starting point, the real benefits of J-RAD are realized with a full-service effort from the JSR Team members.

Full-Service Standards Report. The JSR Team uses this JITC Risk Assessment Methodology to prepare risk assessment reports for full-service customers.

The JSR Team initiates the risk assessment by performing unclassified research in J-RAD and on government and commercial web search engines. The JSR Team forms an initial estimation of likelihood risk factors and creates a spreadsheet, including supporting rationales, that calculates risk based on the accumulated IT standards information. To complete the risk assessment, the JSR customer must review and adjust the risk assessment worksheet using knowledge of system requirements and how the program is implementing the TV-1 standards. The JSR Team will also provide customers with information on test history and resources if known. Every new risk assessment is followed by a J-RAD update to capture the most recent information about the standards.

PURPOSE

This risk assessment methodology provides a step-by-step process for assessing risk in the implementation of standards. Annex A to this appendix contains detailed examples of applying the Risk Assessment Methodology.

RISK ASSESSMENT METHODOLOGY

As stated above, the fundamental risk assessment guidance for the DoD is the "Risk Management Guide for DoD Acquisition." The JSR Team uses this guidance and recommends all JITC testers and AOs also follow it. A link to the DoD Risk Management Guide is also provided in the References section of this document.

The following steps comprise the risk assessment process and are described in detail in the remaining sections.

1. Identify critical implementations of TV-1 standards.
2. Determine value of risk factors for each implementation.
3. Calculate risk for each implementation.

IDENTIFY CRITICAL IMPLEMENTATIONS

Standards are implemented in a system to support activities, functions, and information exchanges. Testers should prepare their Integrated Architecture Traceability Matrix (IATM) before attempting standards testing prioritization. (The IATM methodology is available via the Net-Ready Key Performance Parameter (NR-KPP) Helpdesk wiki at https://www.intelink.gov/wiki/NR-KPP_Helpdesk.) Testers should identify the standards that support critical system functions and information exchanges from the System View-6. Not all TV-1 standards are implemented in support of critical interfaces, functions, or information exchanges and, therefore, have less need to be tested. Only high-risk standard implementations that support joint critical information exchanges may need to be tested. Standard implementations that are low-risk or do not support mission-critical operational activities, functions, or information exchanges do not need to be tested for threshold level compliance with the NR-KPP. Keep in mind that even standard implementations that support critical information exchanges may be low risk due to the relative affect of likelihood as an independent risk factor.

In the system under test, there may be several implementations of each standard. Testers should work with the Program Management Office to associate the standards with their respective system functions and interfaces. Using the system's architecture viewpoints and traceability matrix, testers must identify the discreet list of implementations of the standard in the system's architecture. Specific implementations will identify nodes, interfaces, or information exchanges and correspond to unique identifiers on the system's architecture viewpoints. Specific implementations will correspond to mission functions at the lowest levels of granularity.

Example. Consider how the Command and Control (C2) Information Exchange Data Model (IEDM) standard might be implemented in a Data Aggregator Tool Set. The tester must identify specific, critical implementations of this standard by studying the Tool Set's architecture products. Figure E-1 shows a portion of the Systems View-1 that indicates two implementations (A and B) where C2 IEDM is used to support two critical information exchanges.

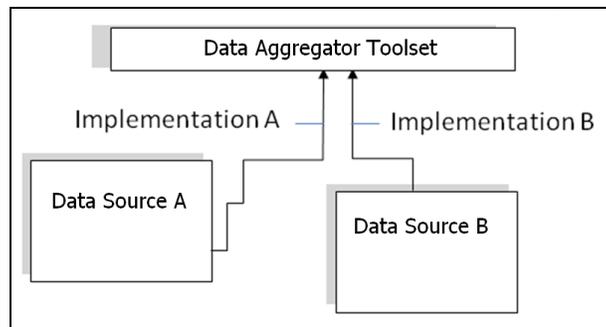


Figure E-1. SV-1 Connections Representing Two Implementations (A and B) of the C2 IEDM Standard

DETERMINE VALUE OF RISK FACTORS

Risk is calculated based on operational impact and likelihood of implementation errors. The test team must consider all known issues (from J-RAD, the Program Office, developer, or other sources) when estimating risk factor values (likelihood and impact).

Known Issues. Known issues are the errors/issues that have occurred in previous implementations of the standard. To accurately calculate risk, testers must consider all known issues for each standard and perform an assessment for each implementation. Testers can only calculate risk based on the issues that have been known to occur. Therefore, the JSR Team must gather as much information as possible about the known issues for IT standards.

The JSR Team accumulates known issues from testers and SMEs and documents them in the J-RAD database. The JSR Team uses the questions listed in Figure E-2 to capture known issues from SMEs.

- How mature/stable is the standard? (A more mature standard will often have a lower likelihood of failure.) What is the Department of Defense Information Technology Standards Registry maturity rating?
- Does the standard have a history of ineffective implementations? What are they?
- Does the standard have a history of problems with other versions, platforms, or standards? What are they?
- Do earlier versions of the system have a history of ineffective implementations of the standard? What was the problem?
- Is this a military-unique standard? (Certain types/categories of standards are less likely to have the same issues that plague commercial developers.)
- Does the standard have a broad support base that will drive continued updates? What organizations comprise the support base?
- Does the developer have experience with the standard?
- For new code:
Was the software developed using a development tool that incorporates the standard and is a mature development tool? (Developers who write code from scratch may not implement the standard correctly.)
- Is the standard dependent on non-mandated standards? What are they?
- Is the standard adaptable? Can the implementation be used through an extended lifespan?
Does the standard have a broad support base that will drive continued updates? What organizations comprise the support base?

Figure E-2. Questions to Provoke Thought about Known Issues

Recall the previous example from Figure E-1. Figure E-3 shows how a tester for the Data Aggregator Tool Set might respond to the questions that provoke thought about known issues (from Figure E-2).

- How mature/stable is the standard? (A more mature standard will often have a lower likelihood of failure.) What is the Department of Defense Information Standards Registry (DISR) maturity rating? **DISR Online states that C2 (Command and Control) Information Exchange Data Model (IEDM) is a mature standard. It has been used as the basis of several other data models, including the Joint Consultation, C2 IEDM, and the C2 Core data models.**
- Does the standard have a history of ineffective implementations? What are they? **Yes. Demos conducted during pilot phase revealed an issue with native schema from a certain provider. The provider changed their schema versioning during testing which caused issues with connectivity.**
- Does the standard have a history of problems with other versions, platforms, or standards? What are they? **No.**
- Do earlier versions of the system have a history of ineffective implementations of the standard? What was the problem? **No.**
- Is this a military-unique standard? **No.**
- Does the standard have a broad support base that will drive continued updates? What organizations comprise the support base? **C2 IEDM has strong support among commercial software vendors.**
- Does the developer have experience with the standard? **Yes.**
- For new code:
Was the software developed using a development tool that incorporates the standard and is a mature development tool? **Not applicable.**
- Is the standard dependent on non-mandated standards? What are they? **No.**

Figure E-3. Questions to Provoke Thought about Known Issues
(Answered for C2 IEDM)

The responses shown in Figure E-3 identify one known issue for the C2 IEDM standard and provide the basis for risk factor estimation in the next steps. We will reuse the responses from those questions as justification and rationale for our likelihood and impact level estimations.

Known Issues Identified for C2 IEDM

1. Version mismatch at information exchange.

Likelihood. Risk varies proportionally with likelihood. The likelihood of each known issue should be estimated using a standard scale. Table E-1 provides the likelihood levels (1 through 5) based on probability of occurrence criteria.

Table E-1. Likelihood Levels

Likelihood Level	Probability of Occurrence Criteria
5	Near Certainty (81-100%)
4	Highly Likely (61-80%)
3	Likely (41-60%)
2	Unlikely (21-40%)
1	Very Unlikely (0-20%)

As a full-service activity, the JSR Team provides an estimate of the likelihood of known issues. The questions listed in Figure E-4 are intended to provoke thought about the likelihood of each known issue. For each known issue, we must consider these questions and, using the criteria in Table E-1, make a determination of likelihood of occurrence (likelihood that the issue will occur).

<p>How likely is the known issue to occur in this implementation?</p> <ul style="list-style-type: none"> • Has the known issue been studied and resolved? • Have resolutions to the known issue been published throughout the developer communities of interest?
--

Figure E-4. Questions to Provoke Thought about Likelihood

Figure E-5 shows how we might respond to the questions that provoke thought about likelihood (from Figure E-4).

<p>How likely is the known issue to occur in this implementation?</p> <ul style="list-style-type: none"> • Has the known issue been studied and resolved? Yes. The version mismatch was discovered and resolved during the data pilot demo. • Have resolutions to the known issue been published throughout the developer communities of interest? Yes. The version mismatch error has been documented and discussed at length during engineering and test planning meetings.

Figure E-5. Questions to Provoke Thought about Likelihood
(Answered for C2 IEDM Known Issue #1)

After considering the questions in Figure E-4, the JSR Team determined the same issue is unlikely to reoccur. According to Table E-1, the resulting likelihood level is 2 (based on the probability of occurrence criteria).

<p>Known Issues Identified for C2 IEDM</p> <ol style="list-style-type: none"> 1. Version mismatch at information exchange. Likelihood = 2
--

Impact. Risk varies proportionally with impact, and criticality is an indication of impact. The impact of each known issue should be estimated using a standard scale. Table E-2 provides the impact levels based on technical performance criteria.

Table E-2. Impact Levels

Impact Level	Technical Performance Criteria
5	Severe degradation in technical performance. Cannot meet key technical threshold. Will jeopardize program success.
4	Significant degradation in technical performance. May jeopardize program success.
3	Moderate reduction in technical performance. Limited impact on program objectives.
2	Minor reduction in technical performance. Can be tolerated with little or no impact on program.
1	Minimal or no consequence to technical performance.

Testers need to think about the standard as it is implemented for each information exchange, node, or system. As information exchanges have varying criticalities, so do the implementations of standards that support them in the operational activities, functions, and nodes.

The questions listed in Figure E-6 are intended to provoke thought about the impact of each known issue. For each known issue, testers must consider these questions and, using the criteria in Table E-2, make a determination of impact of occurrence (impact to the system if the issue were to occur). The JSR Team can assist the testers in considering the impact questions/answers and determining the resulting impact level from the technical performance criteria.

<p>If the known issue occurs, to what degree will it adversely impact the mission or system function?</p> <ul style="list-style-type: none"> • Does this implementation of the standard support a critical function or information exchange? • Does this implementation of the standard enable a joint service? (Does the standard enable access to or by varied Departments, Services, or Agencies?) • Does the implementation affect an information exchange that crosses security or domain boundaries?

Figure E-6. Questions to Provoke Thought about Impact

Figure E-7 shows how a tester for the Data Aggregator Tool Set might respond to the that provoke thought about impact (from Figure E-6).

If the known issue occurs, to what degree will it adversely impact the mission or system function?

- Does this implementation of the standard support a critical function or information exchange?
Yes.
- Does this implementation of the standard enable a joint service?
(Does the standard enable access to or by varied Departments, Services, or Agencies?)
Yes.
- Does the implementation affect an information exchange that crosses security or domain boundaries?
No.

Figure E-7. Questions to Provoke Thought about Impact
(Answered for C2 IEDM Known Issue #1)

After considering the questions in Figure E-6, the test team determines that if the version mismatch issue continues to occur without complete resolution, the system will be unable to meet key performance threshold criteria. According to Table E-2, the resulting impact level is 5 (based on the technical performance criteria).

Known Issues Identified for C2 IEDM

1. Version mismatch at information exchange.
Likelihood = 2 Impact = 5

Some implementations may be immediately marked as low risk (low priority) if the implementation does not support a joint critical information exchange (because the impact would be a 1).

CALCULATE RISK

The DoD Risk Assessment Guide recommends calculating risk according to the Risk Reporting Matrix shown in Figure E-8, where the terms probability and likelihood are synonymous, and the terms impact and consequence are synonymous. The Risk Reporting Matrix illustrates the concept that risk is directly proportional to both likelihood and consequence. Using this matrix, the level of risk is reported as low (green), moderate (yellow), or high (red).

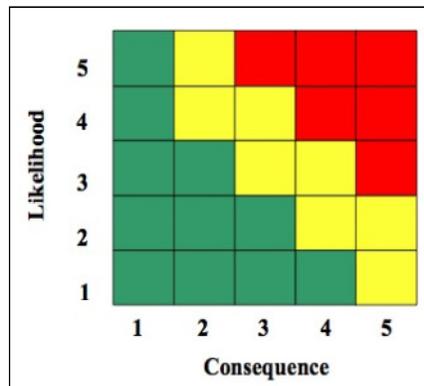


Figure E-8. Risk Reporting Matrix

Likelihood and impact risk factors are independent of each other; i.e., a change in the likelihood of an error will not affect the impact to the operational mission if an error occurs. The final risk value may be altered by changing either risk factor value.

According to the chart, the resulting risk level for the C2 IEDM known issue is in the moderate risk (yellow) range. [Likelihood = 2; Impact = 5.] Notice also that any slight increase in likelihood such as: a lack of communication or publication about the issue, or an incomplete or untested resolution to the issue) will push this issue into the high-risk (red) range. Conversely, impact level would have to drop to 3, "Limited impact on program objectives," before the resulting risk would drop to low. In support of a "full-service" activity, the JSR Team will advise the test team of these considerations so that testers can defend assertions of high or low risk.

Tester Responsibility. The JSR Team provides the Risk Assessment Report and Worksheet as a service intended to help the JITC Action Officer (AO) and tester determine the risk of a given standard or set of standards. This service is not intended to provide the final risk assessment. The intent is to provide the AO and testers with a common starting point for an 80 to 85-percent risk assessment analysis. The AO and tester are responsible for understanding their programs and systems; for understanding how the mandated standards are implemented in the system; and for understanding how known issues might impact their system's operational mission.

The [JITC Guide to Test Documentation](#) instructs testers to include a test methodology description in their test plan and test report. As a full-service activity, the JSR Team will research standards and provide testing advice (to include test tools, laboratories, or test methodologies) when available. This information will be shown in the "Test Tools and Advice" column of the Risk Assessment Worksheet. Multiple test tools and methods may be suggested in the worksheet. In their test plan and test report, testers should describe how the test item will be operated or exercised to determine if it meets requirements. The [JITC Guide to Test Documentation](#) describes the key points that must be addressed and provides detailed guidelines for ensuring proper documentation. Table E-4 shows how the interoperability test report (Table B-6) entry might look for the Data Aggregator Tool Set's C2 IEDM standard.

Table E-3 shows how the risk assessment worksheet would look for one of the Data Aggregator Tool Set's C2 IEDM standard implementations. The black text represents the contents of the worksheet as it might look when it's delivered by the JSR Team to the Data Aggregator Tool Set's test team. The blue text represents the contributions of the test team after considering the impact questions and estimating the impact of the known issue, revising the likelihood according to a better understanding of the issue than is available to the JSR Team, and recalculating the resulting risk. Table E-4 demonstrates how the information in Table E-3 may be represented in Table B-6 of the Interoperability Certification Report.

ANNEX A – EXAMPLE RISK ASSESSMENTS

The following examples are intended to demonstrate how to accomplish step 2 of the Risk Assessment Methodology, "Determine Value of Risk Factors."

VARIABLE MESSAGE FORMAT STANDARDS EXAMPLE

Risk is calculated based on operational impact and likelihood of implementation errors. The test team must consider all known issues (from Joint Interoperability Test Command (JITC) Risk Assessment Database (J-RAD), the Program Office, developer, or other sources) when estimating risk factor values (likelihood and impact).

Known Issues. To accurately calculate risk, testers must consider all known issues for each standard and perform an assessment for each implementation. Testers can only calculate risk based on the issues that have been known to occur. Therefore, the JITC Standards Research (JSR) Team must gather as much information as possible about the known issues for Information Technology (IT) standards.

Figure E-A-1 shows how the known issue questions might be answered in regards to two Variable Message Format (VMF) standards.

- How mature/stable is the standard? (A more mature standard will often have a lower likelihood of failure.) What is the Department of Defense Information Technology Standards Registry (DISR) maturity rating?
DISR indicates this standard is mature and readily available.
- Does the standard have a history of ineffective implementations? What are they?
Yes. Variable Message Format (VMF) implementations are known to experience frequent issues related to version mismatch, especially between Services. The Army and the United States Marine Corps do not use the same implementation of the standards for some messages.
- Does the standard have a history of problems with other versions, platforms, or standards? What are they?
Yes. Messages from different baselines are not compatible. The VMF Baseline and the Header version must match.
- Do earlier versions of the system have a history of ineffective implementations of the standard? What was the problem?
No.
- Is this a military-unique standard?
No.
- Does the standard have a broad support base that will drive continued updates? What organizations comprise the support base?
Yes. Most, if not all, of the Armed Forces support implementation of this standard.
- Does the developer have experience with the standard?
Yes.
- For new code:
Was the software developed using a development tool that incorporates the standard and is a mature development tool?
Not applicable.
- Is the standard dependent on non-mandated standards? What are they?
No.

Figure E-A-1. Questions to Provoke Thought about Known Issues
(Answered for MIL-STD-6017A)

The responses shown in Figure E-A-1 identify one known issue for Military Standard 6017A (MIL-STD-6017A), VMF standard and provide the basis for risk factor estimation in the next steps. We will reuse the responses from those questions as justification and rationale for our likelihood and impact level estimations.

Likelihood. As a full-service activity, the JSR Team provides an estimate of the likelihood of known issue(s). Figure E-A-2 shows how the likelihood questions might be answered in regards to MIL-STD-6017A known issue #1.

- | |
|---|
| <p>Known Issues Identified for MIL-STD-6017A</p> <ol style="list-style-type: none"> 1. Messages from different baselines are not compatible. The VMF Baseline and the Header version must match. 2. The Army and the USMC do not use the same implementation of the standards for some messages. |
|---|

How likely is the known issue to occur in this implementation?

- Has the known issue been studied and resolved?
Yes.
- Have resolutions to the known issue been published throughout the developer communities of interest?
Yes. The version mismatch errors have been documented and discussed at length.

Figure E-A-2. Questions to Provoke Thought about Likelihood (Answered for MIL-STD-6017A Known Issue #1)

After considering the likelihood questions, the JSR Team has determined that the same issue is unlikely to reoccur. The resulting likelihood level is 2.

Impact. The JSR Team can assist the testers in considering the impact questions/answers and determining the resulting impact level from the technical performance criteria.

Figure E-A-3 shows how a tester might respond to the impact questions in regards to MIL-STD-6017A known issue #1.

Known Issues Identified for VMF

1. Messages from different baselines are not compatible. The VMF Baseline and the Header version must match.
Likelihood = 2
2. The Army and the USMC do not use the same implementation of the standards for some messages.
Likelihood = 3

If the known issue occurs, to what degree will it adversely impact the mission or system function?

- Does this implementation of the standard support a critical function or information exchange?
Yes.
- Does this implementation of the standard enable a joint service?
(Does the standard enable access to or by varied Departments, Services, or Agencies?)
Yes.
- Does the implementation affect an information exchange that crosses security or domain boundaries?
No.

Figure E-A-3. Questions to Provoke Thought about Impact (Answered for MIL-STD-6017A Known Issue #1)

After considering the impact questions, the test team determines that if the version mismatch issue continues to occur without complete resolution, the system will be unable to meet key performance threshold criteria. The resulting impact level is 5.

According to the chart, the resulting risk level for the MIL-STD-6017A known issue #1 is in the moderate risk (yellow)

Known Issues Identified for VMF

1. Messages from different baselines are not compatible. The VMF Baseline and the Header version must match.
Likelihood = 2 Impact = 5
2. The Army and the USMC do not use the same implementation of the standards for some messages.
Likelihood = 3 Impact = 3

range. [Likelihood = 2; Impact = 5.] Notice also that any slight increase in likelihood (such as: 1) a lack of communication or publication about the issue, OR 2) an incomplete or untested resolution to the issue) will push this issue into the high-risk (red) range. Conversely, impact level would have to drop to 3, "Limited impact on program objectives," before the resulting risk would drop to low. In support of a "full-service" activity, the JSR Team will advise the test team of these considerations so that testers can defend assertions of high or low risk.

Table E-A-1 shows how the risk assessment worksheet might look for two VMF standards. The black text represents the contents of the worksheet as it might look when it's delivered by the JSR Team to the test team. The blue text represents the contributions of the test team after considering the impact questions and estimating the impact of the known issues, revising the likelihood according to a better understanding of the issue than is available to the JSR Team, and recalculating the resulting risk. Table E-A-2 shows how the interoperability test report (Table B-6) entry might look for MIL-STD-2045-47001D(1) 1C.

Table E-A-1. Example Risk Assessment Worksheet showing VMF Standards

Service Area	Standard ID	Standard Title	DISR	Critical Interface (Yes or No)	Known Issues	Test Tools and Advice	Summary of Standard	Supporting Rationale for Likelihood	Supporting Rationale for Impact	Likelihood	Impact	Risk
Provide tactical information	MIL-STD-6017A	Variable Message Format (VMF)	Mandated	Yes	Known Issue 1: Messages from different baselines are not compatible. The VMF Baseline and the Header version must match. Known Issue 2: The Army and the USMC do not use the same implementation of the standards for some messages	No known test tools/ methods	The C2 IEDM is a common data model to facilitate exchange of information in context with the coalition partners through command and control systems.	DISR indicates this standard is mature and readily available. However, known issues 1 & 2 apply to this implementation.	May jeopardize program success. A work-around is available.	2	4	Moderate
Provide tactical information	MIL-STD-2045-47001D(1) 1C	Connectionless Data Transfer Application Layer Standard	Mandated	Yes	Known Issue 1: Messages from different baselines are not compatible. The VMF Baseline and the Header version must match. Known Issue 2: The Army and the USMC do not use the same implementation of the standards for some messages	No known test tools/ methods	The C2 IEDM is a common data model to facilitate exchange of information in context with the coalition partners through command and control systems.	DISR does not provide a maturity rating. However, known issues 1 & 2 apply to this implementation.	May jeopardize program success. A work-around is available.	4	4	High
<p>NOTES:</p> <p>1. Black indicates the initial contributions made by the JSR Team.</p> <p>2. Blue indicates the additions and adjustments made by the Test Team.</p> <p>LEGEND:</p> <p>DISR Department of Defense Information Technology Standards Registry JSR JITC Standards Research ID Identification MIL-STD Military Standard JITC Joint Interoperability Test Command USMC United States Marine Corps</p>												

Table E-A-2. Suggested Entry in Table B-6 of the Interoperability Certification Report

Service Area	Standard Identifier	Title of Standard	DISR Status	Risk/Rationale (See Note 1)	Evaluation Method	Status
Document Interchange	MIL-STD-2045-47001D(1) 1C	Connectionless Data Transfer Application Layer Standard	Mandated	High Risk – Version mismatch errors are common, especially between Services.	Observation during Interoperability Test. No standards conformance issues were noted.	Met
<p>LEGEND:</p> <p>DISR Department of Defense Information Technology Standards Registry MIL-STD Military Standard</p>						

HYPertext MARKUP LANGUAGE 4.0.1 STANDARD EXAMPLE

Risk is calculated based on operational impact and likelihood of implementation errors. The test team must consider all known issues (from J-RAD, the Program Office, developer, or other sources) when estimating risk factor values (likelihood and impact).

Known Issues. To accurately calculate risk, testers must consider all known issues for each standard and perform an assessment for each implementation. Testers can only calculate risk based on the issues that have been known to occur. Therefore, the JSR Team must gather as much information as possible about the known issues for IT standards.

Figure E-A-4 shows how the known issue questions might be answered in regards to the HyperText Markup Language (HTML) 4.0.1 standard.

- How mature/stable is the standard? (A more mature standard will often have a lower likelihood of failure.) What is the Department of Defense Information Technology Standards Registry (DISR) maturity rating?
DISROnline states that Hypertext Markup Language (HTML) 4.0.1 is mature and publicly available.
- Does the standard have a history of ineffective implementations? What are they?
No.
- Does the standard have a history of problems with other versions, platforms, or standards? What are they?
No.
- Do earlier versions of the system have a history of ineffective implementations of the standard? What was the problem?
Yes. HTML 4.0.1 documents are not displayed properly when used with certain browsers or applications.
- Is this a military-unique standard?
No.
- Does the standard have a broad support base that will drive continued updates? What organizations comprise the support base?
Yes. HTML 4.0.1 has strong support among commercial developers.
- Does the developer have experience with the standard?
Yes.
- For new code:
Was the software developed using a development tool that incorporates the standard and is a mature development tool?
Not applicable.
- Is the standard dependent on non-mandated standards? What are they?
No.

Figure E-A-4. Questions to Provoke Thought about Known Issues
(Answered for the HTML 4.0.1 Standard)

The responses shown in Figure E-A-4 identify one known issue for the HTML 4.0.1 standard and provide the basis for risk factor estimation in the next steps. We will reuse the responses from those questions as justification and rationale for our likelihood and impact level estimations.

Known Issues Identified for HTML 4.0.1

1. HTML 4.0.1 documents are not displayed properly when used with certain browsers or applications.

Likelihood. As a full-service activity, the JSR Team provides an estimate of the likelihood of known issue(s). Figure E-A-5 shows how the likelihood questions might be answered in regards to HTML 4.0.1 standard.

How likely is the known issue to occur in this implementation?

- Has the known issue been studied and resolved?
No. It remains a common problem with certain browsers.
- Have resolutions to the known issue been published throughout the developer communities of interest?
Yes.

Figure E-A-5. Questions to Provoke Thought about Likelihood
(Answered for HTML 4.0.1 Known Issue #1)

After considering the likelihood questions, the JSR Team has determined that the same issue is likely to reoccur. The resulting likelihood level is 3. Likelihood of error depends on history of success with the browsers used in the HTML implementations in the system under test. If the program uses one of the problem browsers or applications, then it would be more likely that implementation errors would occur. In that case, the test team would enter a high likelihood level (such as a 4 or a 5) and provide justification in the “Supporting Rationale for Likelihood” column.

Known Issues Identified for HTML 4.0.1

1. HTML 4.0.1 documents are not displayed properly when used with certain browsers or applications.
Likelihood = 3

Impact. The JSR Team can assist the testers in considering the impact questions/answers and determining the resulting impact level from the technical performance criteria.

Figure E-A-6 shows how a tester might respond to the impact questions in regards to the HTML 4.0.1 standard.

If the known issue occurs, to what degree will it adversely impact the mission or system function?

- Does this implementation of the standard support a critical function or information exchange?
Yes. This implementation enables a high-priority command and control system. If the standard is implemented improperly or fails to allow usable display of critical information on the hypertext markup language document, then the system will not meet threshold performance criteria.
- Does this implementation of the standard enable a joint service?
(Does the standard enable access to or by varied Departments, Services, or Agencies?)
Yes.
- Does the implementation affect an information exchange that crosses security or domain boundaries?
No.

Figure E-A-6. Questions to Provoke Thought about Impact
(Answered for HTML 4.0.1 Known Issue #1)

After considering the impact questions, the test team determines that if the issue continues to occur without complete resolution, the system will be unable to meet key performance threshold criteria. The resulting impact level is 5.

According to the chart, the resulting risk level for the HTML 4.0.1 known issue is in the high risk (red) range. [Likelihood = 3; Impact = 5.]

**Known Issues Identified for HTML
4.0.1**

1. HTML 4.0.1 documents are not displayed properly when used with certain browsers or applications.
Likelihood = 3
Impact = 5

Table E-A-3 shows how the risk assessment worksheet would look for the HTML 4.0.1 standard. The black text represents the contents of the worksheet as it might look when it's delivered by the JSR Team to the test team. The blue text represents the contributions of the test team after considering the impact questions and estimating the impact of the known issues, revising the likelihood according to a better understanding of the issue than is available to the JSR Team, and recalculating the resulting risk. Table E-A-4 shows how the interoperability test report (Table B-6) entry might look for HTML 4.0.1.

Table E-A-3. Example Risk Assessment Worksheet showing HTML 4.0.1 Standard

Service Area or Implementation	Standard ID	Standard Title	DISR Status	Critical Interface (Yes or No)	Known Issues	Test Tools and Advice	Summary of Standard	Supporting Rationale for Likelihood	Supporting Rationale for Impact	Likelihood Level	Impact Level	Risk																
Document Interchange	HTML 4.0.1	HTML 4.0.1 Specification, W3C Recommendation, revised, 24 Dec 1999	Mandated	Yes	HTML 4.0.1 is known to experience compatibility issues with some web browsers and applications.	Test capability: Instrumentation Group/Net-Centric Test Lab Test tools: W3C Markup Validation Service, WDG HTML Validator, A Real validator Test Methodology: Available in J-RAD	This specification defines the HTML, the publishing language of the World Wide Web.	DISR Technical Maturity statement indicates this standard is mature and publicly available. However, some testers have reported compatibility issues with some web browsers and applications. Although compatibility issues have been reported with some web browsers and applications, none of the problem browsers or applications are known to be used with this implementation.	This implementation enables a high-priority C2 system. If the standard is implemented improperly or fails to allow usable display of critical information on the HTML document, then the system impact will be: Cannot meet key performance threshold. Will jeopardize program success.	3 2	5	Moderate																
<p>NOTES:</p> <p>1. Black indicates the initial contributions made by the JSR Team. The strike-through text represents information that might be deleted.</p> <p>2. Blue indicates the additions and adjustments made by the Test Team.</p> <p>LEGEND:</p> <table border="0"> <tr> <td>C2</td> <td>Command and Control</td> <td>J-RAD</td> <td>JITC Risk Assessment Database</td> </tr> <tr> <td>DISR</td> <td>Department of Defense Information Technology Standards Registry</td> <td>JSR</td> <td>JITC Standards Research</td> </tr> <tr> <td>HTML</td> <td>HyperText Markup Language</td> <td>W3C</td> <td>World Wide Web Consortium</td> </tr> <tr> <td>JITC</td> <td>Joint Interoperability Test Command</td> <td>WDG</td> <td>Web Design Group</td> </tr> </table>													C2	Command and Control	J-RAD	JITC Risk Assessment Database	DISR	Department of Defense Information Technology Standards Registry	JSR	JITC Standards Research	HTML	HyperText Markup Language	W3C	World Wide Web Consortium	JITC	Joint Interoperability Test Command	WDG	Web Design Group
C2	Command and Control	J-RAD	JITC Risk Assessment Database																									
DISR	Department of Defense Information Technology Standards Registry	JSR	JITC Standards Research																									
HTML	HyperText Markup Language	W3C	World Wide Web Consortium																									
JITC	Joint Interoperability Test Command	WDG	Web Design Group																									

Table E-A-4. Suggested Entry in Table B-6 of the Interoperability Certification Report

Service Area	Standard Identifier	Title of Standard	DISR Status	Risk/Rationale (See Note 1)	Evaluation Method	Status								
Document Interchange	HTML 4.0.1 Specification	HTML 4.0.1 Specification, W3C Recommendation, revised, 24 Dec 1999	Mandated	Moderate Risk - Widely used, well established commercial standard.	Validated with the W3C Markup Validation Service, met all requirements	Met								
<p>LEGEND:</p> <table border="0"> <tr> <td>DISR</td> <td>Department of Defense Information Technology Standards Registry</td> <td>W3C</td> <td>World Wide Web Consortium</td> </tr> <tr> <td>HTML</td> <td>HyperText Markup Language</td> <td></td> <td></td> </tr> </table>							DISR	Department of Defense Information Technology Standards Registry	W3C	World Wide Web Consortium	HTML	HyperText Markup Language		
DISR	Department of Defense Information Technology Standards Registry	W3C	World Wide Web Consortium											
HTML	HyperText Markup Language													

SIMPLE MAIL TRANSFER PROTOCOL STANDARD EXAMPLE

Risk is calculated based on operational impact and likelihood of implementation errors. The test team must consider all known issues (from J-RAD, the Program Office, developer, or other sources) when estimating risk factor values (likelihood and impact).

Known Issues. To accurately calculate risk, testers must consider all known issues for each standard and perform an assessment for each implementation. Testers can only calculate risk based on the issues that have been known to occur. Therefore, the JSR Team must gather as much information as possible about the known issues for IT standards.

Figure E-A-7 shows how the known issue questions might be answered in regards to the Simple Mail Transfer Protocol (SMTP) standard, Internet Engineering Task Force Request for Comment (IETF RFC) 1870.

- How mature/stable is the standard? (A more mature standard will often have a lower likelihood of failure.) What is the Department of Defense Information Technology Standards Registry (DISR) maturity rating?
DISROnline states that the standard is mature and publicly available.
- Does the standard have a history of ineffective implementations? What are they?
No, but success of Internet Protocol version 6 with this standard has not been proven.
- Does the standard have a history of problems with other versions, platforms, or standards? What are they?
No.
- Do earlier versions of the system have a history of ineffective implementations of the standard? What was the problem?
No.
- Is this a military-unique standard?
No.
- Does the standard have a broad support base that will drive continued updates? What organizations comprise the support base?
Yes. The standard has strong support among commercial developers.
- Does the developer have experience with the standard?
Yes.
- For new code:
Was the software developed using a development tool that incorporates the standard and is a mature development tool?
Not applicable.
- Is the standard dependent on non-mandated standards? What are they?
No.

Figure E-A-7. Questions to Provoke Thought about Known Issues
(Answered for the SMTP standard, IETF RFC 1870)

Known Issues Identified for IETF RFC 1870

1. Success of IPv6 with this standard has not been proven.

The responses shown in Figure E-A-7 identify one known issue for IETF RFC 1870 and provide the basis for risk factor estimation in the next steps. We will reuse the responses from those questions as justification and rationale for our likelihood and impact level estimations.

Likelihood. As a full-service activity, the JSR Team provides an estimate of the likelihood of known issue(s). Figure E-A-8 shows how the likelihood questions might be answered in regards to IETF RFC 1870.

How likely is the known issue to occur in this implementation?

- Has the known issue been studied and resolved?
No, but this implementation does not use Internet Protocol version 6.
- Have resolutions to the known issue been published throughout the developer communities of interest?
No.

Figure E-A-8. Questions to Provoke Thought about Likelihood
(Answered for IETF RFC 1870)

After considering the likelihood questions, the JSR Team has determined that this issue is not possible since Internet Protocol version 6 (IPv6) is not used. The resulting likelihood level is 1. If the program used IPv6, then it would be more likely that implementation errors would occur. In that case, the test team would enter a higher likelihood level (such as a 3, 4, or a 5) and provide justification in the "Supporting Rationale for Likelihood" column.

Known Issues Identified for IETF RFC 1870

1. Success of IPv6 with this standard has not been proven.
Likelihood = 1

Impact. The JSR Team can assist the testers in considering the impact questions/answers and determining the resulting impact level from the technical performance criteria.

Figure E-A-9 shows how a tester might respond to the impact questions in regards to IETF RFC 1870.

If the known issue occurs, to what degree will it adversely impact the mission or system function?

- Does this implementation of the standard support a critical function or information exchange?
Yes, but this implementation enables an objective (not threshold) requirement.
- Does this implementation of the standard enable a joint service?
(Does the standard enable access to or by varied Departments, Services, or Agencies?)
Yes.
- Does the implementation affect an information exchange that crosses security or domain boundaries?
No.

Figure E-A-9. Questions to Provoke Thought about Impact
(Answered for IETF RFC 1870 Known Issue #1)

After considering the impact questions, the test team determines that if the issue were to occur and the standard was implemented improperly, then the system impact would be: Minor reduction in performance. The resulting impact level is 2.

**Known Issues Identified for
IETF RFC 1870**

1. Success of IPv6 with this standard has not been proven.
Likelihood = 1
Impact = 2

According to the chart, the resulting risk level for the IETF RFC 1870 known issue is in the low risk (green) range. [Likelihood = 1; Impact = 2.]

Table E-A-5 shows how the risk assessment worksheet would look with the IETF RFC 1870 standard. The black text represents the contents of the worksheet as it might look when it's delivered by the JSR Team to the test team. The blue text represents the contributions of the test team after considering the impact questions and estimating the impact of the known issues, revising the likelihood according to a better understanding of the issue than is available to the JSR Team, and 3) recalculating the resulting risk. Table E-A-6 shows how the interoperability test report (Table B-6) entry might look for IETF RFC 1870.

Table E-A-5. Example Risk Assessment Worksheet for IETF RFC 1870

Service Area or Implementation	Standard ID	Standard Title	DISR Status Critical Interface (Yes or No)	Known Issues	Test Tools and Advice	Summary of Standard	Supporting Rationale for Likelihood	Supporting Rationale for Impact	Likelihood Level	Impact Level	Risk																
Electronic Mail	IETF RFC 1870	Simple Mail Transfer Protocol Services Extension for Message Size Declaration, November 1995	Mandated Yes	Success of IPv6 with this standard has not been proven.	No test methodology provided.	This memo defines an extension to the SMTP service whereby an SMTP client and server may interact to give the server an opportunity to decline to accept a message (perhaps temporarily) based on the client's estimate of the message size.	DISR Technical Maturity statement indicates this standard is mature and publicly available. However, specific implementation should be considered when estimating the likelihood of failure. A system using IPv6 with this standard will have a higher likelihood of failure due to lack of proven use. Although issues may occur with IPv6, this implementation will only be used with IPv4.	This implementation enables an objective requirement. If the standard is implemented improperly or prevents usability, then the system impact will be: Minor reduction in performance. Can be tolerated with little or no impact on program.	1	2	Low																
<p>NOTES:</p> <p>1. Black indicates the initial contributions made by the JSR Team. The strike-through text represents information that might be deleted.</p> <p>2. Blue indicates the additions and adjustments made by the Test Team.</p> <p>LEGEND</p> <table> <tr> <td>DISR</td> <td>Department of Defense Information Technology Standards Registry</td> <td>JSR</td> <td>JITC Standards Research</td> </tr> <tr> <td>IETF</td> <td>Internet Engineering Task Force</td> <td>RFC</td> <td>Request For Comment</td> </tr> <tr> <td>IPv</td> <td>Internet Protocol version</td> <td>SMTP</td> <td>Simple Mail Transfer Protocol</td> </tr> <tr> <td>JITC</td> <td>Joint Interoperability Test Command</td> <td></td> <td></td> </tr> </table>												DISR	Department of Defense Information Technology Standards Registry	JSR	JITC Standards Research	IETF	Internet Engineering Task Force	RFC	Request For Comment	IPv	Internet Protocol version	SMTP	Simple Mail Transfer Protocol	JITC	Joint Interoperability Test Command		
DISR	Department of Defense Information Technology Standards Registry	JSR	JITC Standards Research																								
IETF	Internet Engineering Task Force	RFC	Request For Comment																								
IPv	Internet Protocol version	SMTP	Simple Mail Transfer Protocol																								
JITC	Joint Interoperability Test Command																										

TO BE MOVED TO THE “NR-KPP Guidebook” Acronym List

ACRONYMS

AO	Action Officer
C2	Command and Control
DISA	Defense Information Systems Agency
DISR	Department of Defense Information Technology Standards Registry
DoD	Department of Defense
HTML	HyperText Markup Language
IATM	Integrated Architecture Traceability Matrix
IEDM	Information Exchange Data Model
IETF RFC	Internet Engineering Task Force Request for Comment
IPv6	Internet Protocol version 6
IT	Information Technology
JITC	Joint Interoperability Test Command
J-RAD	JITC Risk Assessment Database
JSR	JITC Standards Research
MIL-STD	Military Standard
NR-KPP	Net-Ready Key Performance Parameter
SME	Subject Matter Expert
TV	Technical View
VMF	Variable Message Format

(This page intentionally left blank.)

TO BE MOVED TO THE "NR-KPP Guidebook" Reference List

REFERENCES

DEPARTMENT OF DEFENSE DOCUMENTS

"Risk Management Guide for DoD Acquisitions Sixth Edition." Version 1.0, August 2006. Pertinent material taken from Section 4, "Key Activity - Risk Analysis," pp. 11-17, <http://www.dau.mil/pubs/gdbks/docs/RMG%20Ed%20Aug06.pdf>

DISA DOCUMENTS

"The JITC Guide to Test Documentation." June 2008.
https://jitcnet.fhu.disa.mil/policy_letters/guidetstdoc.pdf

(This page intentionally left blank.)