JITC Standards Research (JSR) Team

J-RAD 102

This briefing is UNCLASSIFIED

Shaina Williams (AO)
Kevin McComish (TL)

May 2012

Version 0.1

DISA
A Combat Support Agency

Agenda

- JSR Team Overview
- JSR Available Services
- J-RAD 102 Overview
- JITC Risk Assessment Methodology
  - 1. Identify critical implementations of TV-1 standards
  - 2. Determine value of risk factors
  - 3. Calculate risk for each implementation
- Next steps for testers
  - Test plan
  - Test report

JSR Team Overview

- JITC Standards Risk Assessment Methodology
  - NR-KPP Guidebook, Appendix E
  - http://jitc.fhu.disa.mil/cgi/jsr/
- J-RAD population and maintenance
  - Standards research
- JITC Standards Research (JSR) Services Available
  - Full Service
  - Self Service

DISA
A Combat Support Agency

JSR Available Services

- J-RAD Self-service
  - Instructions for access: http://jitc.fhu.disa.mil/cgi/jsr/downloads/jsr_request.pdf
  - New web-enabled J-RAD Self Service
- J-RAD Full-service
  - Estimate level of risk
  - Prioritize testing
  - Justification for priority of testing
  - Rationale to support testing decisions
  - Plan for test resources
- JSR Other Services

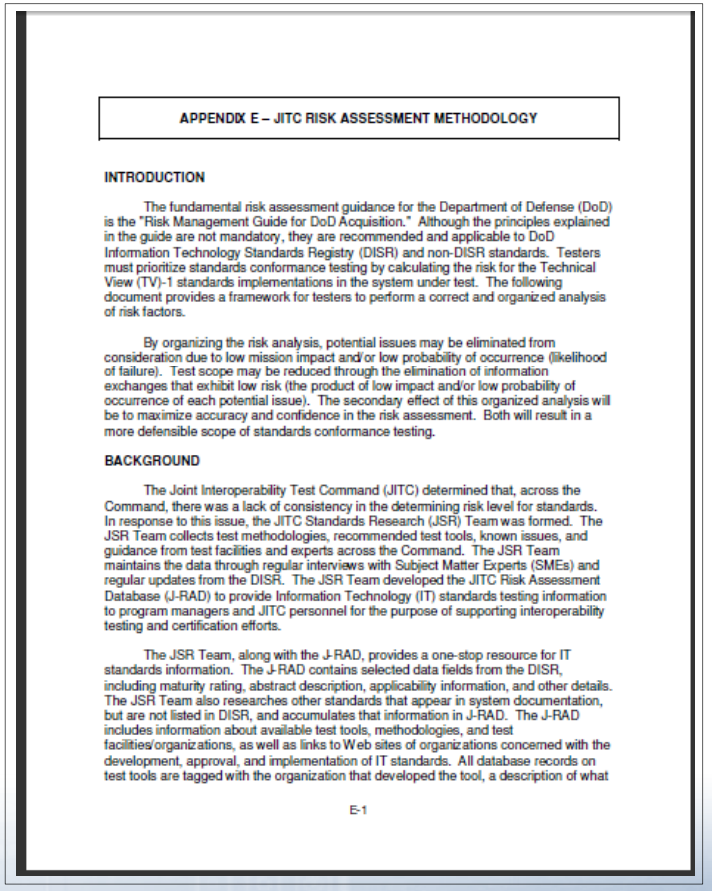
DISA
A Combat Support Agency

J-RAD 102 Overview

- To provide a complete understanding of the standards risk assessment methodology as published in the NR-KPP Guidebook – Appendix E
- To give testers the ability to perform critical thinking necessary to identify known issues and consider the implications for their system with respect to likelihood of failure and impact of potential failure.
- To provide a standardized set of quantification levels necessary to estimate the value of risk factors for their standards implementations in context with the system under test.

JITC Risk Assessment Methodology

- Follows DoD Risk Methodology
  - http://www.dau.mil/pubs/gdbks/docs/RMG 6Ed Aug06.pdf
- Accurate Risk Calculation
- Promotes development of supporting rationale (for defensible test plans)



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

E-1

JITC Risk Assessment Methodology

1. Identify critical implementations of TV-1 standards

Technical Standards View (TV-1)
Standards Profile for AUTOMATIC IDENTIFICATION SYSTEM

DISR System Profile: TV-1 for Navy Automatic Identification System
System Description: This TV-1 standards profile is for AIS Increment 1 on U.S. Navy shore, surface, and subsurface platforms.
System Classification: Unclassified
Created by: Scott Thompson
Published Date: 2009-09-23
CDD or ISP Stage 1: yes

Technical Standards View (TV-1) - The Technical Standards Profile collects the various systems standards rules that implement and sometimes constrain the choices that can be made in the design and implementation of an architecture.

IT Profile: Navy AIS
IT Description: This TV-1 profile includes the probable and possible standards applicable to AIS on Navy ships and platforms.
IT Profile Classification: Unclassified
Last Updated: 2009-09-23

Service Area	Standard Identifier	Title of Standard	Published Status	Sun-set	Current Status	Sun-set
Military Messaging	ANSI/IEEE 754	Binary Floating-Point Arithmetic, March 21, 1985	Mandated		Mandated	
Document Interchange	CISS GJXDM	Global Justice XML Data Model, Version 3.0.3	Mandated		Mandated	
Document Interchange	CISS ISM: XML	Common Information Sharing Standard for Information Security Marking: XML Implementation, Implementation Guide, Release 2.0.3, 15 February 2006	Mandated		Mandated	
Authentication	CMS/XML Digital Signature Profiles v1.1	DoD Digital Signature Implementation Profiles	Mandated		Mandated	
Application-Oriented (GPS)	ICD-GPS-227	Navstar GPS Selective Availability and Anti-Spoofing (SA/A-S) Host Application Equipment (HAE) Design Requirements with the Selective Availability Anti-Spoofing Module (SAASM), 26 November 2003	Mandated		Mandated	
C4ISR: Payload Platform	IEEE 1394	High Performance Serial Bus, December 1995	Mandated		Mandated	
C4ISR: Payload Platform	IEEE 1394a	High Performance Serial Bus, Attachment 1, 2000	Mandated		Mandated	
Network Technologies	IEEE 802.1X:2004	Local and Metropolitan Area Networks - Port Based Network Access Control	Mandated		Mandated	
Network Technologies	IEEE 802.3-2005	Local and Metropolitan Area Networks - Specific Requirements, Part 3: Carrier Sense Multiple Access with Collision	Mandated		Mandated	

2. Determine value of risk factors

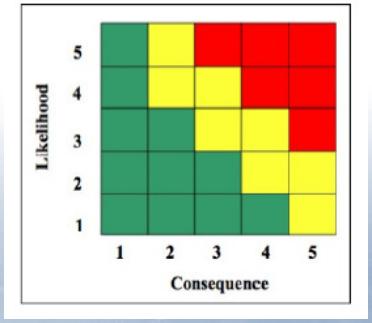
Table E-1. Likelihood Levels

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%)

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.

3. Calculate risk for each implementation



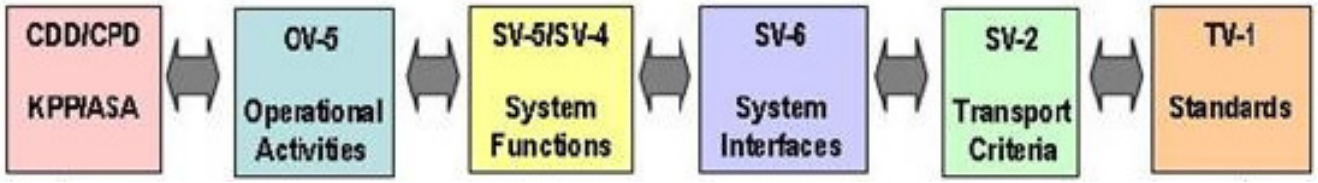
1. Identify critical implementations

- Review the System View-6

Interface Identifier	Data Exchange Identifier	Data Description							Producer		Consumer		Nature of Transaction			
System Interface Name and Identifier	System Data Exchange Name and Identifier	Data Element Name and Identifier	Content	Format Type	Media Type	Accuracy	Units of Measurement	Data Standard	Sending System Name and Identifier	Sending System Function Name and Identifier	Receiving System Name and Identifier	Receiving System Function Name and Identifier	Transaction Type	Triggering Event	Interoperability Level Achieved	Criticality

Interface Identifier	Data Exchange Identifier	Performance Attributes				Information Assurance						Security				
System Interface Name and Identifier	System Data Exchange Name and Identifier	Periodicity	Timeliness	Throughput	Size	Access Control	Availability	Confidentiality	Dissemination Control	Integrity	Non-Repudiation Producer	Non-Repudiation Consumer	Protection (Type Name, Duration, Date)	Classification	Classification Caveat	Releasability	Security Standard

- Create an Integrated Architecture Traceability Matrix



- Standard implementations that need to be tested:
  - Implementations that support joint critical information exchanges
  - Implementations that support joint critical system functions

DISA
A Combat Support Agency

2. Determine value of risk factors

- Identify and consider known issues
- Estimate and quantify likelihood that implementation will fail
- Estimate and quantify potential impact of failure

DISA
A Combat Support Agency

2. Determine value of risk factors

- Identify known issues
  - 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.)

2. Determine value of risk factors

- Identify known issues (Cont.)
  - 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?

DISA
A Combat Support Agency

2. Determine value of risk factors

- Estimate and quantify likelihood
  - Has the known issue been studied and resolved?
  - Have resolutions to the known issue been published throughout the developer communities of interest?

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%)

DISA
A Combat Support Agency

2. Determine value of risk factors

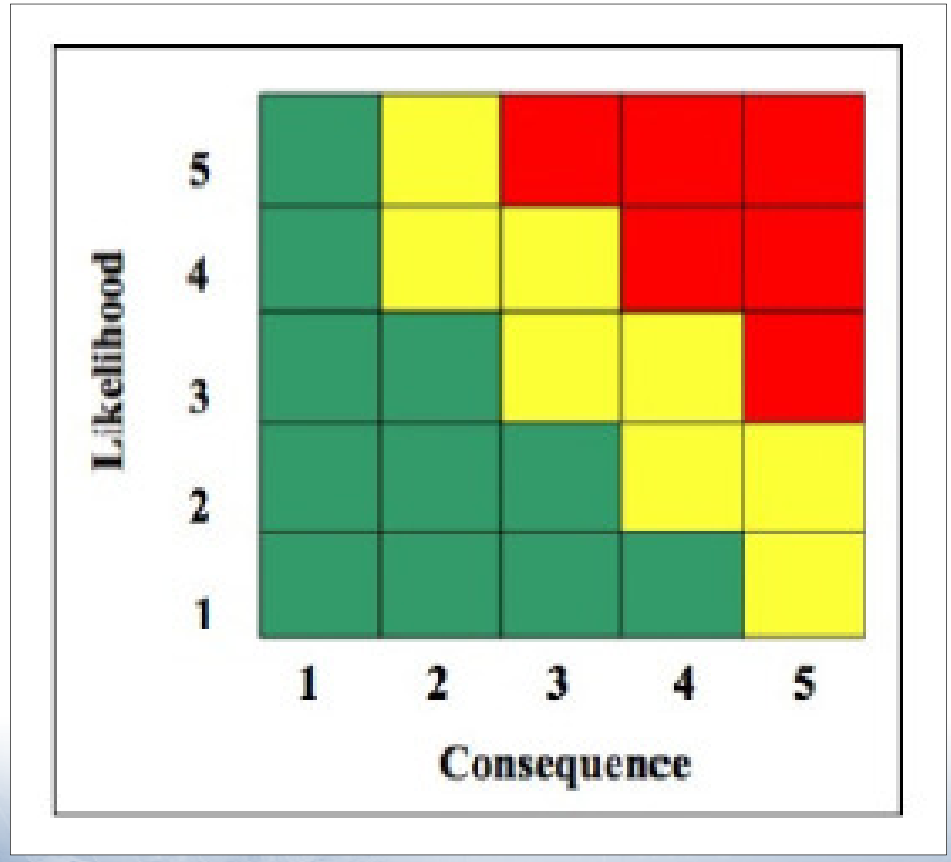
- Estimate and quantify impact
  - Does this implementation of the standard support a critical function or information exchange?
  - Does this implementation of the standard enable a joint service?
  - Does the standard enable access to or by varied Departments, Services, or Agencies?
  - Does the implementation affect an information exchange that crosses security or domain boundaries?

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.

DISA
A Combat Support Agency

3. Calculate risk

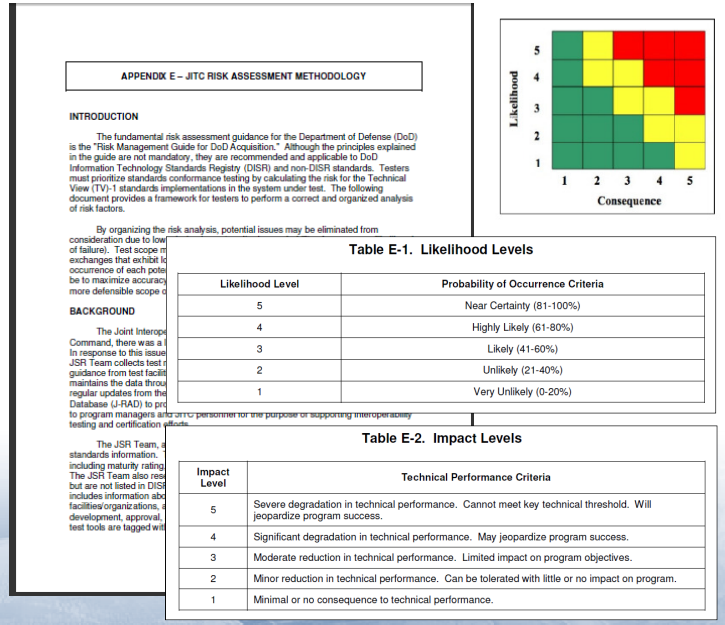
- Use risk matrix as shown in the DoD Risk Assessment Guide



DISA
A Combat Support Agency

Next steps for testers

- Plan testing to focus on high risk implementations
  - Defend test plan using quantifiable risk with rationales
- Report test results
  - Defend untested implementations using quantifiable risk with rationales



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

of failure). Test scope m

exchanges that exhibit lo

occurrence of each poten

be to maximize accuracy

more defensible scope o

BACKGROUND

The Joint Interope

Command, there was a

In response to this issue

JSR Team collects test r

guidance from test facilit

maintains the data throu

regular updates from the

Database (J-RAD) to pro

to program managers and JITC personnel for the purpose of supporting interoperability

testing and certification efforts.

The JSR Team,

standards information.

including maturity rating

The JSR Team also rese

but are not listed in DISR

includes information abo

facilities/organizations,

development, approval,

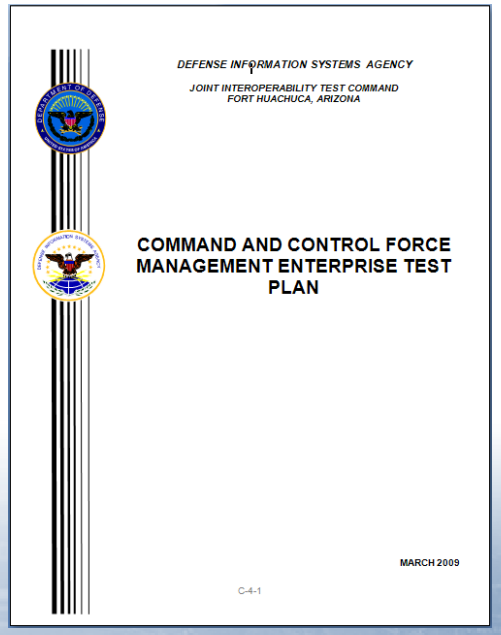
test tools are tagged wit

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%)

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.



DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

COMMAND AND CONTROL FORCE MANAGEMENT ENTERPRISE TEST PLAN

MARCH 2009

C-4-1

DISA
A Combat Support Agency

Summary

- Estimate level of risk
- Prioritize testing
- Justification for priority of testing
- Justification to support testing decisions
- Plan for test resources
- Benefits
  - Follows DoD Risk Methodology
  - Accurate Risk Calculation
  - Promotes development of supporting rationale (for defensible test plans)

DISA
A Combat Support Agency

Helpful Links

- JSR Page on JITC website
  - http://jitc.fhu.disa.mil/cgi/jsr/
- JSR Methodology
  - http://jitc.fhu.disa.mil/cgi/jsr/downloads/nrkpp_guidebook_appdxe.pdf
- Submit a JSR Request
  - http://jitc.fhu.disa.mil/cgi/jsr/#
- NR-KPP Guidebook
  - https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=347416

DISA

A Combat Support Agency

DEFENSE INFORMATION SYSTEMS AGENCY

Version 0.1