

# Introduction to the KBSI Activity Model of the Cybersecurity Test & Evaluation Guidebook Process



Knowledge Based Systems, Inc.



# Activity Model Reference

- KBSI has developed an activity model of the process described in the Cybersecurity Test & Evaluation Guidebook as a reference framework for locating and understanding cybersecurity modeling, support, and evaluation tools.
  - The IDEF-0 activity model formalism was used for this modeling activity ([www.idef.com](http://www.idef.com)).
  - The viewpoint taken in the modeling effort was that of the policy analyst or decisionmaker being addressed as the audience of the Guidebook.

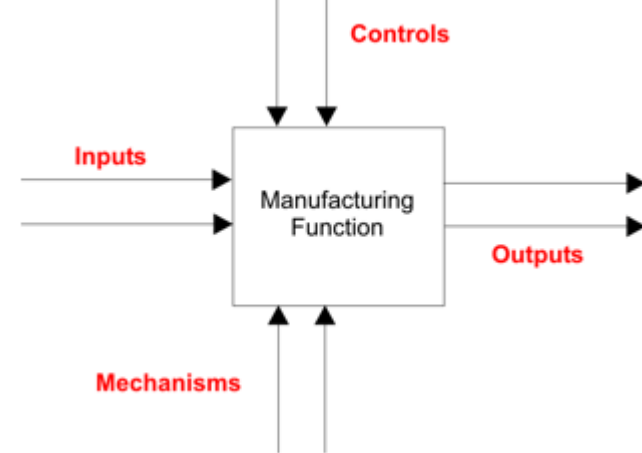


# Cybersecurity Test and Evaluation Guidebook

- "The purpose of [DoD Cybersecurity Test and Evaluation Guidebook] is to promote data-driven mission-impact-based analysis and assessment methods for cybersecurity test and evaluation (T&E) and to support assessment of cybersecurity, system cyber survivability, and operational resilience within a mission context by encouraging planning for tighter integration with traditional system T&E. Cybersecurity T&E starts at acquisition initiation and continues throughout the entire life cycle." [Guidebook pg 1]



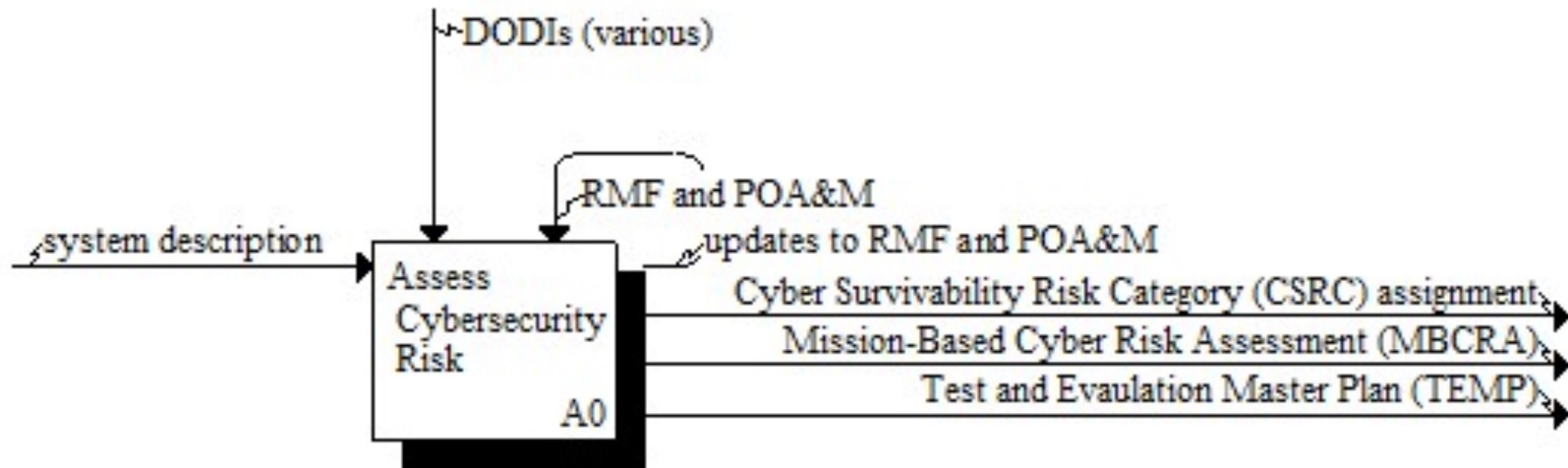
# Reading the Activity Model



- IDEF-0 portrays activities and their interdependencies.
  - Activities are depicted as rectangular boxes
  - The resources that interconnect activities (called *flows*) are depicted as directional arrows.
- Each activity is shown as having four types of interaction:
  - Inputs – entities that are consumed during execution of the activity
  - Controls – entities that determine the execution of the activity
  - Outputs – entities that are produced (either originally or through modification) as a result of execution of the activity
  - Mechanisms – resources that either mechanize execution of the activity or serve as a reference base during execution.



# Reading the Activity Model



- In the diagram above
  - The depicted activity is named "Assess Cybersecurity Risk" and has the activity number "A0" (by convention, the number used for the root, or top, activity)
  - This activity is controlled by "DODIs (various)" and "RMF and POA&M"
  - The activity uses as input the "system description"
  - The activity produces as output
    - "updates to RMF and POA&M"
    - "Cyber Survivability Category (CSRC) assignment"
    - "Mission-Based Cyber Risk Assessment (MBCRA)"
    - "Test and Evaluation Master Plan (TEMP)"



# Navigating the Model on this Site

The outline in the left window lists all of the activities in the model. Clicking on an item in the left-hand window will cause descriptive material for that item to appear in the right-hand window

## ASSURANT Direct Use (OBE)

### Assess Cyber-based Risk

#### A0: Assess Cyber-based Risk

#### Manage Models

#### A1: Manage Models

#### Create New Model

#### A11: Create New Model

#### Create Empty Model

#### Import Pre-existing Model

#### Import System Description Data

#### Add or Edit Model Elements

#### A12: Add or Edit Model Elements

#### Compare Models

#### Construct System Component Model

#### A122: Construct System Component Model

#### Select Components

#### Fill Out Component Data Sheet

#### Interconnect Model Elements

#### Identify Entry Points

#### Identify Vulnerabilities, Threats, and Impacts

#### Model Missions

#### Evaluate Model

#### Perform Analyses

#### A2: Perform Analyses

#### Generate visual summaries

#### Manage Cyber Survivability

#### A22: Manage Cyber Survivability

#### Identify Mitigation Opportunities

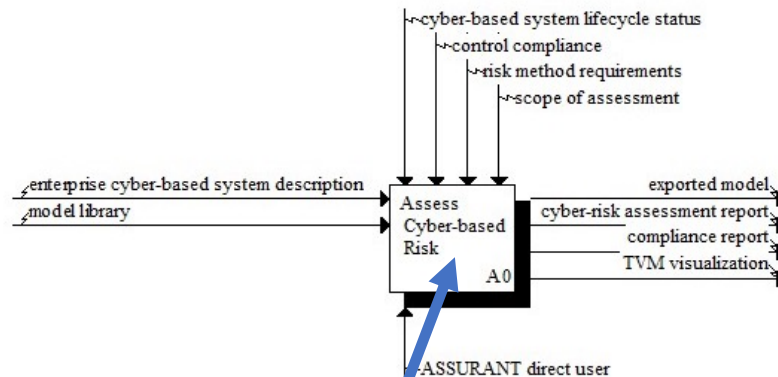
#### Estimate Mitigation Cost and Time

#### Provide Risk-response Investment Decision Support

#### Generate analytics

#### A23: Generate analytics

## Model: ASSURANT Direct Use (OBE)



**Creator** Tim Ramey

### **Purpose:**

This model explores the usage

### **Context:**

ASSURANT is a suite of tools

ASSURANT direct user intera

### **Viewpoint:**

Direct user of ASSURANT

### **Description**

## Activities

### Assess Cyber-based Risk

## Concepts

cyber-based system lifecycle status

enterprise cyber-based system description

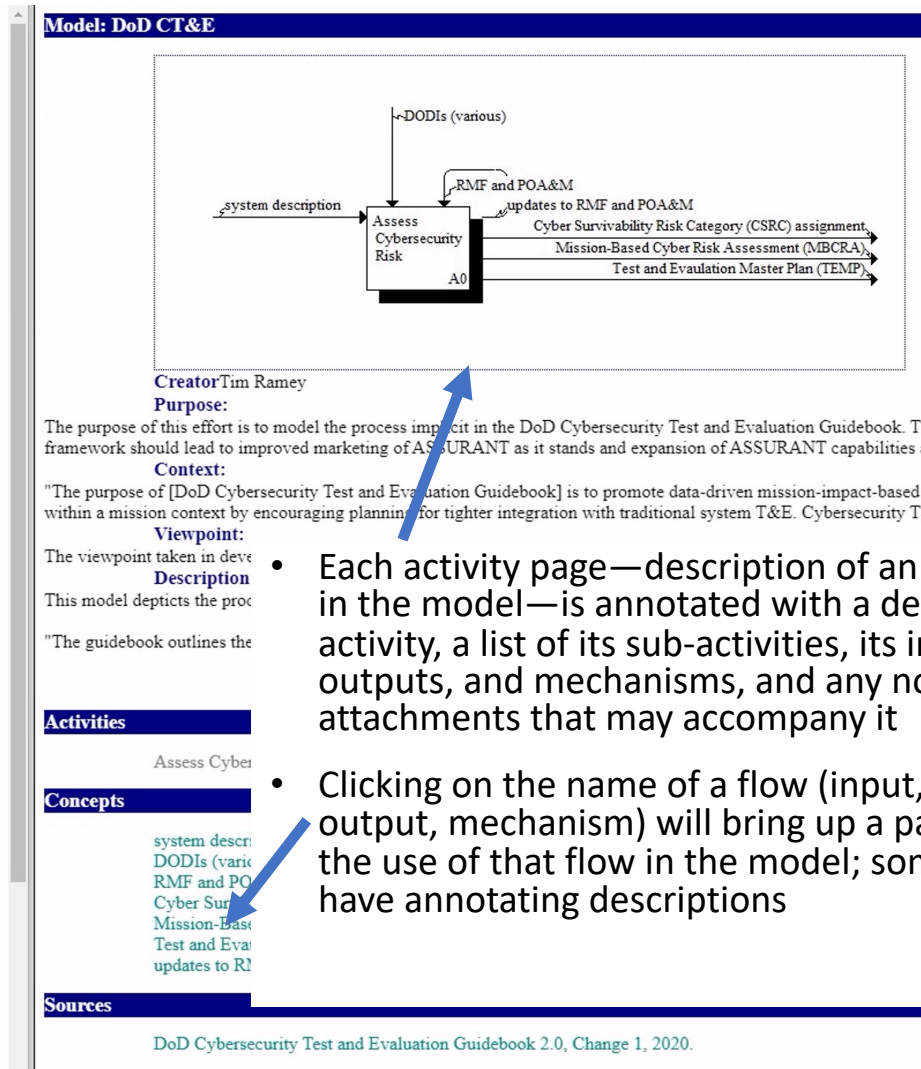
- Each activity page—description of an activity node in the model—is annotated with a description of the activity, a list of its sub-activities, its inputs, controls, outputs, and mechanisms, and any notes and attachments that may accompany it
- Clicking on the name of a flow (input, control, output, mechanism) will bring up a page showing the use of that flow in the model; some flows do not have annotating descriptions



# Navigating the Model on this Site

The outline in the left window lists all of the activities in the model. Clicking on an item in the left-hand window will cause descriptive material for that item to appear in the right-hand window

A0: Assess Cybersecurity Risk  
Phase 1: Understand Cyber Security Requirements  
A1: Phase 1: Understand Cyber Security Requirements  
Compile Cybersecurity Requirements and Security Resources  
A11: Compile Cybersecurity Requirements and Security Resources  
Examine Cybersecurity Standards  
Examine Operational Resilience Requirements  
Examine System Cybersurvivability Requirements  
Prepare for Phase 3 & 4 DT&E  
A12: Prepare for Phase 3 & 4 DT&E  
Develop the Initial DEF  
A121: Develop the Initial DEF  
Define Security Capabilities  
Determine Evaluation Data Needed  
Determine Test Activities Needed  
Incorporate Test Activities into Test Events and Document  
Identify Supporting Cybersecurity T&E Resources  
Develop the Initial OT Evaluation Framework  
Align RMF Artifacts with the TEMP  
Align DCO Activities to Support the RMF  
Plan and Schedule MBCRA  
Develop Cybersecurity T&E Strategy  
Phase 2: Characterize Attack Surface  
A2: Phase 2: Characterize Attack Surface  
Identify the Cyber-attack Surface  
A21: Identify the Cyber-attack Surface  
Examine System Architecture, Components, and Data Flows  
A211: Examine System Architecture, Components, and Data Flows  
Identify System Components and Interaction Entities  
Create Attack Surface List  
Identify Key Terrain  
Analyze and Decompose System Mission  
Map Mission Dependencies  
Examine Roles and Responsibilities  
Analyze the Attack Surface  
A22: Analyze the Attack Surface  
Characterize the Cyber Threat  
Select a Cyber Kill Chain  
Examine Cyber Effects on System and Mission  
Perform or Update MBCRA  
Document Results and Update Test Planning and Artifacts  
A23: Document Results and Update Test Planning and Artifacts  
Document Results of Cyber-Attack Surface Analysis



- Each activity page—description of an activity node in the model—is annotated with a description of the activity, a list of its sub-activities, its inputs, controls, outputs, and mechanisms, and any notes and attachments that may accompany it
- Clicking on the name of a flow (input, control, output, mechanism) will bring up a page showing the use of that flow in the model; some flows do not have annotating descriptions





# Navigating the Model on this Site

- Each activity is depicted on two pages
  - A descriptive page
  - A diagram page
- On the descriptive page
  - Click 'Owning Diagram' to see the diagram of the parent activity
  - Click under 'Decomposition' to see the diagram for this activity
- On the diagram page
  - Click on an activity node to see the descriptive page for that activity
  - Click on a link below the diagram to see the description of that entity

## Activity-in-Diagram: Compile Cybersecurity Requirements and Security Resources

Creator: Tim Ramey

### Description

"As early and as often as possible, the CyWG reviews system documentation to extract: 1) cybersecurity standards, system cyber survivability, and operational resilience requirements; 2) information that may influence test conditions, environments, or methods; and 3) information that may influence the prioritization of testing. The CyWG ensures that the requirements are testable, measurable, and achievable." [Guidebook]

See Guidebook Table 4.1

Owning Diagram A1: Phase 1: Understand Cyber Security Requirements

### Decomposition

A11: Compile Cybersecurity Requirements and Security Resources

### Output

catalog of cybersecurity resources  
Cyber Survivability Risk Category (CSRC) assignment  
catalog of cybersecurity requirements

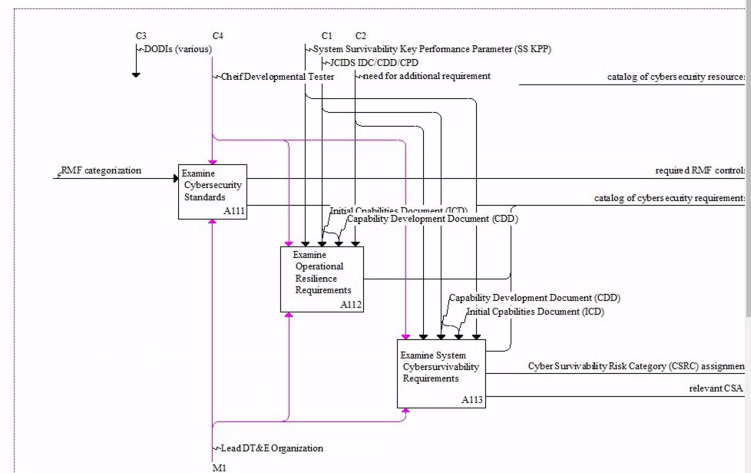
### Control

JCIDS IDC/CDD/CPD  
need for additional requirement  
DODIs (various)  
Chief Developmental Tester

### Mechanism

Lead DT&E Organization

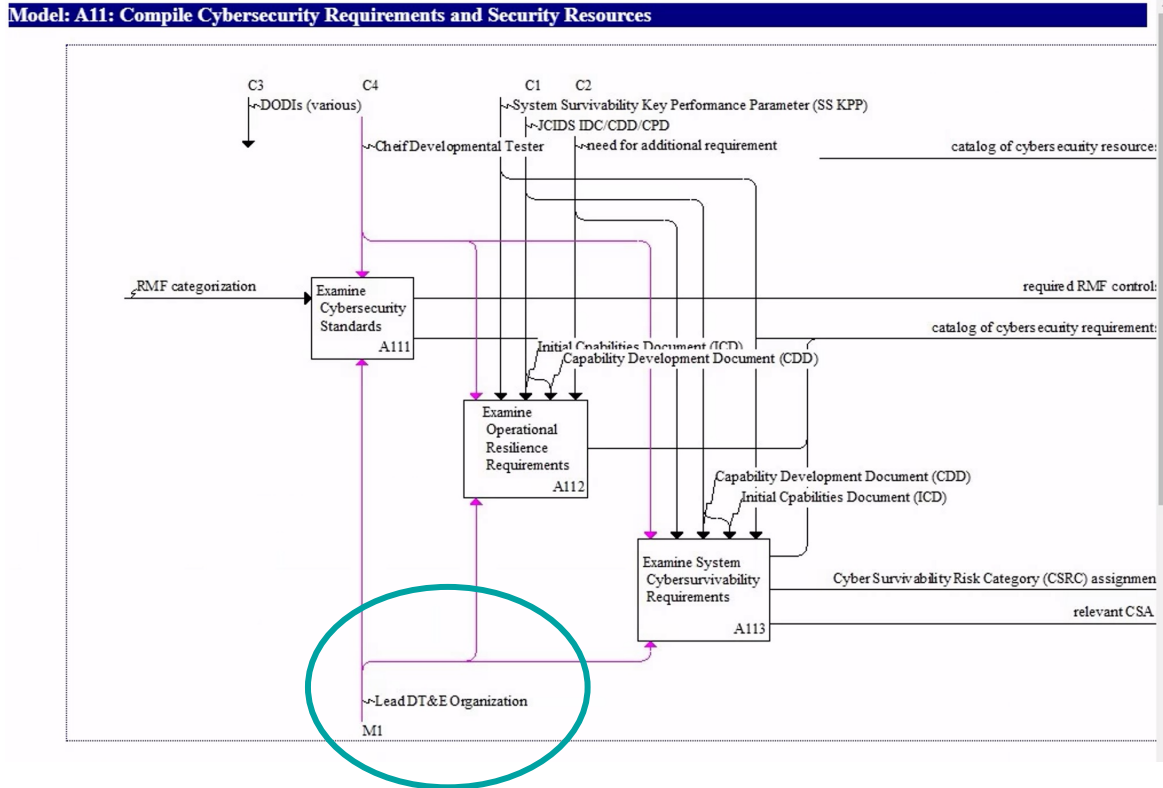
## Model: A11: Compile Cybersecurity Requirements and Security Resources







# Special Annotations on the Model



- Flows shown in a magenta color are performer resources—personnel or organizations
  - Performers identified in the Guidebook as 'accountable' in an activity are shown as controls
  - Performers identified in the Guidebook as 'responsible' in an activity are shown as mechanisms



# Please Send Us: Comments, Recommendations, Criticisms

- At the bottom of each page will be found a link for sending feedback to the model author
  - "Send Feedback"
  - Clicking on that link will open an e-mail composition window in which you can write your comment
  - The e-mail is pre-addressed and contains information in the 'subject' line that allow the model author to know which page you are looking at
  - Include in your comment any orienting information necessary to focus the model author's attention to the part of the diagram you are commenting on
- The author may not be able to respond to each comment, but every comment is appreciated and is an opportunity for improvement