INSTITUTE FOR DEFENSE ANALYSES

A Cross-Reference of Mission-Based Cyber Risk Assessment (MBCRA) Inputs and Outputs

Rachel Kuzio de Naray, Project Leader
Allyson M. Buytendyk, Principal Author

March 2022
IDA Document P-32941
Log: H 2022-000010

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001, Project AX-1-3100, Technical Analysis for the Director, Developmental Test, Evaluation and Assessments. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

The authors would like to thank the IDA committee, Dr. Stephen M. Ouellette (chair), Dr. Rhiannon T. Hutton, Dr. Davy Y. Lo and Dr. Tye W. Botting, for providing technical review of this effort.

For More Information

John S. Hong, Project Leader
jhong@ida.org, 703-845-2564

Stephen M. Ouellette, Director, SED
souellet@ida.org, 703-845-2443

Copyright Notice

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-32941

A Cross-Reference of Mission-Based Cyber Risk Assessment (MBCRA) Inputs and Outputs

Rachel Kuzio de Naray (Project Leader)

Allyson M. Buytendyk (Principal Author)

Executive Summary

Mission based cyber risk assessments (MBCRAs) are methodologies used to identify, estimate, assess and prioritize cybersecurity risks for hardware and information systems being employed in operations. Department of Defense instruction (DoDI) 5000.89 "Test and Evaluation" requires acquisition programs conduct MBCRAs throughout a system's developmental life cycle to ensure planning for cybersecurity measures takes into consideration real-world context. Current Department of Defense (DoD) policy, however, does not provide any guidance on how to evaluate the quality of MBCRA methodologies; nor does it define specific criteria to examine, or results that must be generated by MBCRAs, to inform system security decisions.

Using previous Institute for Defense Analyses (IDA) work in consultation with MBCRA source documentation in this study facilitated the development of reference of common MBCRA data inputs and output formats, across the active methodologies. This paper provides an analysis of the commonalities between MBCRAs available to the DoD community, to help inform evaluation criteria for MBCRA methodologies to support testing.

Findings

- Nearly 50 percent of the active MBCRAs are *Collaborative* methodologies that bring together program, cyber intelligence, and other subject matter experts in a team-based assessment exercise.
- The Fourth Estate (DoD Agencies) and Federally Funded Research and Development Centers (FFRDC)/University Affiliated Research Centers (UARC) have developed many of the active MBCRAs; the services have each created one or more methodology of their own.
- Eleven types of required data inputs are common to the active MBCRAs. Of these 11, three relate to the mission, five are system-specific, and three characterize the adversarial threat.
  - Test-Integrated methodologies (which use test data to evaluate risk) do not include any of the common required data inputs for the mission.
  - Control/Compliance methodologies (which assess the risk to a system due to previously identified vulnerabilities and non-compliant controls) do not include any of the common required data inputs for the threat.

- Five output formats are common to how most of the active MBCRAs report risk results.
  - Mission-Separable methodologies (which allow mission- and system-level analyses to be performed independently) do not report risk results using any of the common output formats.
- Each of the common required data inputs map to at least one of the common risk reporting output formats for the active MBCRAs.

Recommendations

- The MBCRA descriptive categories offer a way to distinguish methodologies at a high-level but should not be used to evaluate their quality.
- Methodologies should include analysis of the mission, system and threat to be classified as MBCRAs.
- Analysis of the common input information across methodologies compared to the acquisition life cycle time frame could help inform MBCRA policy.
- MBCRA outputs (e.g., types of risk representation) that are most valuable and inform better designs should be evaluated when defining criteria.

Contents

Table of Figures

1. Introduction

Mission based cyber risk assessments (MBCRAs) are methodologies used to identify, estimate, assess and prioritize cybersecurity risks[1] for hardware and information systems being employed in operations. Department of Defense instruction (DoDI) 5000.89 "Test and Evaluation" requires acquisition programs conduct MBCRAs throughout a system's developmental life cycle, to ensure planning for cybersecurity measures takes into consideration real-world context.[2] Current Department of Defense (DoD) policy, however, does not provide any guidance on how to evaluate the quality of MBCRA methodologies; nor does it define specific criteria to examine or results that must be generated by MBCRAs to inform system security decisions. Programs are left to decide which of the more than 25 methodologies developed by or for DoD to use that aligns with their information, resource, and schedule constraints.

In 2017, the Institute for Defense Analyses (IDA) reviewed 20 methodologies and developed a decision scheme to help programs select an MBCRA.[3] Ambroso and Hutton define six descriptive categories to group the methodologies: mission separable, test-integrated, capabilities-based, collaborative, control/compliance and modeling for simulation, defined as follows:

- *Mission-separable* methodologies allow potential reuse of common mission threats for different systems because mission- and system-level analyses can be performed independently.
- *Test-integrated* methodologies incorporate test data to evaluate risk.
- *Capabilities-based* methodologies use catalogs/databases of capabilities (offense and defensive) to determine risk, relative costs and benefits of proposed mitigations.
- *Collaborative* methodologies bring together program, cyber intelligence, and other subject matter experts in a team-based assessment exercise.

[1] NIST SP 800-60 Vol. 1 Rev. 1 defines cybersecurity risk as an effect of uncertainty on or within information and technology.

[2] Department of Defense Instruction (DoDI) 5000.89 "Test and Evaluation," November 19, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF?ver=Plc85E0-NVNide91K3XQLA%3D%3D

[3] Ambroso, Michael and Rhiannon Hutton, Comparative Review of DoD Mission-Based Cyber Risk Assessments, Alexandria, VA: Institute for Defense Analyses, P-8736, February 2018.

- *Control/compliance* methodologies assess the risk to a system due to previously identified vulnerabilities and non-compliant controls.
- *Modeling for simulation* methodologies build representative mission, system, and adversary models and then execute simulated attacks and analyze the outcomes to assess risk.

Then the authors compiled an analysis, for each category, which compares individual methodology information constraints or required data inputs, resources, and desired outputs to help users select an MBCRA based on their available data. The category types paired with the individual methodology analysis formed the basis of the MBCRA Decision Diagram, which guided users through a series of questions relevant to acquisition programs to help them select the MBCRA most appropriate for their needs. IDA published an update to the initial review of MBCRAs in 2020 in which five of the original methodologies were found inactive (i.e., no longer in use); the 2020 report also incorporated six new methodologies.[4] De Naray and Galvin categorized and summarized the new methodologies, updated seven previous methodologies, and updated the comparison tables from the 2017 report.

We revisited these earlier studies and their source documentation to develop a reference of the common required data inputs and output formats for the methodologies specified as active[5] in 2020. This paper provides an analysis of the commonalities between DoD MBCRAs, to inform evaluation criteria for MBCRA methodologies to aid the testing community.

[4] de Naray, Rachel K. and Keith Galvin, Comparative Review of DoD MBCRAs: 2020 Updates and New Methodologies, Alexandria, VA: Institute for Defense Analyses, P-14309, September 2020.

[5] For this paper the definition for an active MBCRA is a current methodology or the most recent version available.

2. MBCRA Cross-Reference

A. Methodologies by Category

The descriptive categories developed by IDA highlight major differences between methodological approaches and offer a quick way to identify which type of MBCRA might be suitable for a user's needs.[6] In 2017, no more than 30 percent of the methodologies reviewed were in a single category, with the *Collaborative* type having the highest count. With the 2020 classification of several methodologies as inactive and addition of several others, the total number of MBCRAs remains the same;[7] however, the distribution of methodologies across categories skews further to the *Collaborative* type. Close to half of the active MBCRAs considered in this paper are in the *Collaborative* category. Figure 1 illustrates the shift in types of methodologies reviewed in 2017 and 2020 among the six descriptive categories.

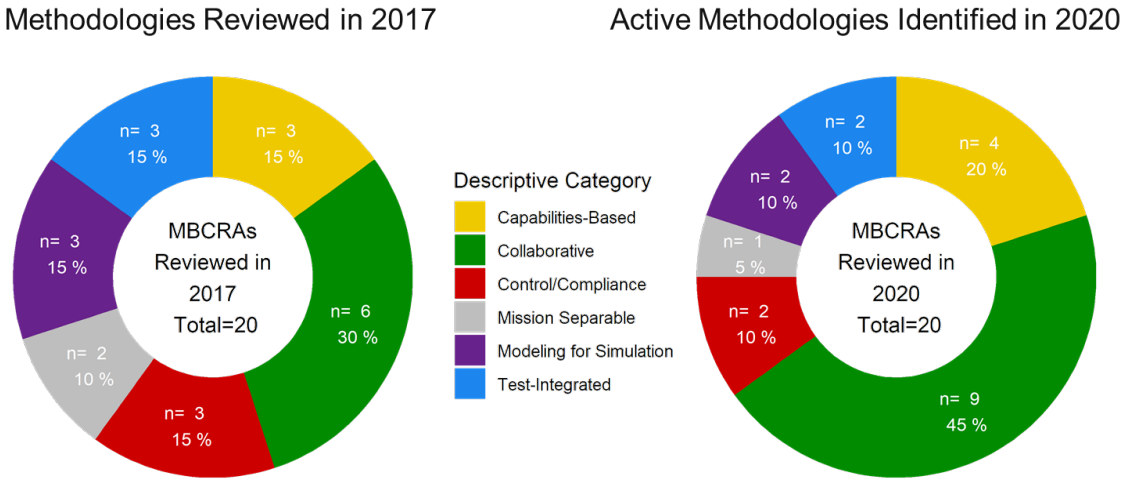

Figure 1. Comparison of MBCRAs by descriptive methodology category from 2017 to 2020.

[6] "When methodologies possessed attributes of more than one category, they were assigned to the category that the authors believed best represented their intended purpose," (Ambroso 2017).

[7] Two of the new methodologies identified in 2020 were noted as frameworks and grouped together in the review since the authors noted the approaches were undergoing refinement. For this analysis, we consider that group of two as one new MBCRA. This reduces the number of specified new MBCRAs reported in 2020 by one, from six to five, and with five identified as inactive, brings the total number to 20.

The four military services as well as the Fourth Estate (DoD agencies) have embraced MBCRA-like approaches for test and evaluation of systems for more than 20 years. The DoD community has produced its own approaches; DoD has also sponsored Federally Funded Research and Development Centers (FFRDCs) or University Affiliated Research Centers (UARCs) to develop methodologies. Additionally, other government agencies have created their own cyber risk assessment methodologies for their own missions. Figure 2 shows the breakdown of active MBCRAs considered in this paper by the organization that developed the methodology and descriptive category. The Fourth Estate and FFRDC/UARC developed many of the methodologies in use; that said, each of the services has created one or more.

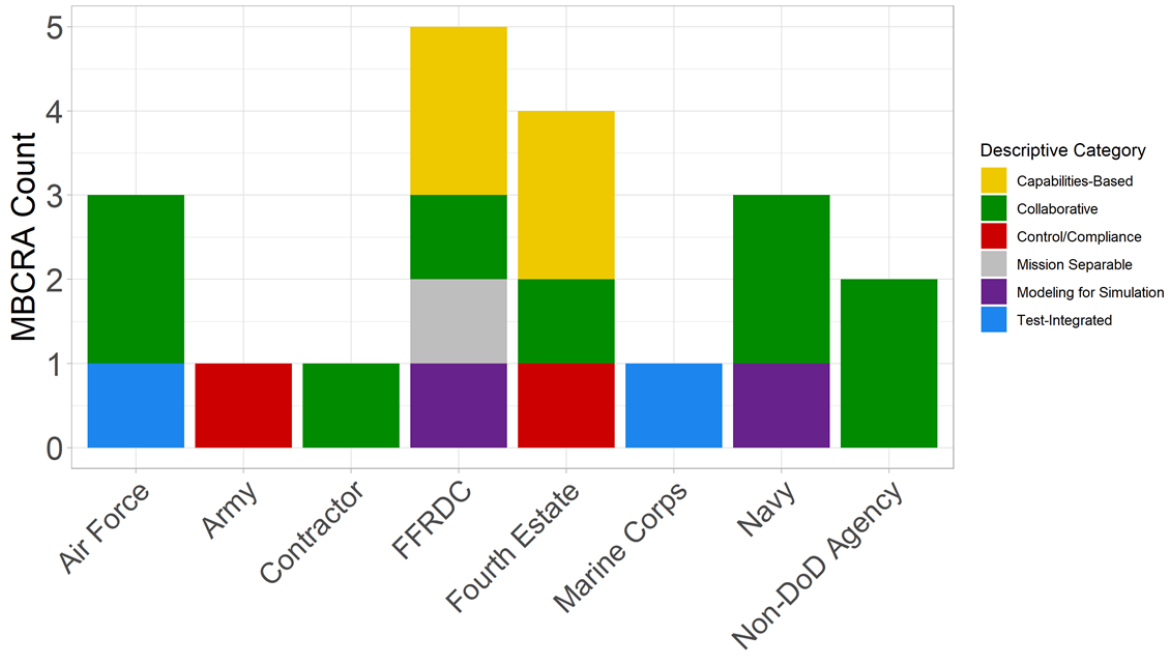

Figure 2. Summary of 20 active MBCRAs identified in 2020 by type of organization that developed the methodology.

B. Required Data Inputs

IDA examined some of the data inputs required for each MBCRA in their previous analyses. Those comparison tables generated in 2017 and updated in 2020, however, only highlight notable differences between the individual MBCRAs, within a specific category type. That is, the comparison tables do not represent *all* the required data inputs for the MBCRAs.

For this analysis, we used these previously identified required data inputs for the 20 active MBCRAs as a starting point and then reviewed the source documentation to collect a complete set of input requirements across the methodologies. Since many methodologies

involve multiple process steps and/or stages of analysis, we define "required input data" as user supplied reference information (e.g., diagrams, documents, etc.) or facts that exist prior to the assessment and are necessary to conduct an MBCRA. For instance, the process for one methodology is to generate a list of vulnerabilities using previous test data, so the test data are the required input data. Another methodology involves assigning risk to specific system components using a list of vulnerabilities from an open source search, so in this case the list of vulnerabilities is the required input data. Alternatively, a software based MBCRA already contains a database of known vulnerabilities as part of the methodology to graph the system risk over time so the user does not need to supply the information.

From the set of required data inputs, we gathered on all 20 active MBCRAs, we defined those shared by 25 percent or more (i.e., at least 5 out of 20) of the methodologies as the common inputs for MBCRAs. Using this definition, we identified 11 common required data inputs and found that 80 percent (i.e., 16 out of 20) of the MBCRAs have required data inputs that pertain to the mission, the system, and the adversary or threat.

The 11 common required data inputs represent our interpretation of the descriptions found in the source material and the basis for using the information in the methodology since many MBCRAs refer to similar concepts but use varying terminology.

- **Mission**
  - Core Mission Description – a high-level description that defines the mission.
  - Threads / Operational Tasks – specific scenarios or steps outlined to complete the mission.
  - Mission Decomposition – a list of assets and capabilities for specific mission functions.
- **System**
  - System Architecture – diagrams or documentation that show boundaries and connections (e.g., interfaces, nodes, etc.) between artifacts in the system or sub-system.
  - Component Information – data about artifacts in the system (e.g., controls, maintenance procedure, etc.)
  - Essential Functions – specific system function(s) critical to the mission or scenario.
  - Data / Protocol Flow Diagrams – documentation that shows information flow and/or information exchange boundaries.
  - Mitigations (planned / in place) – procedures for artifacts during specific scenarios (e.g., cyber-attack, system failures, etc.)

- **Threat**
  - Means / Capability – the adversary's technical ability or resources for a cyber-attack.
  - Opportunity / Tactics – the adversary's cyber-attacks or countermeasures.
  - Motive / Intent – the adversary's reason or objective to attack.

Summary of MBCRA required inputs by theme: There are two MBCRAs that do not require data inputs about the mission in their methodologies and these are in the *Test-Integrated* MBCRA descriptive category. There are also two MBCRAs that do not require data inputs that characterize the adversary or level of cyber threat and these are in the *Control/Compliance* MBCRA descriptive category. Unsurprisingly, all the MBCRAs require data inputs about the system. Figure 3 depicts the proportion of MBCRAs by theme (mission, system, threat) of common required data inputs.

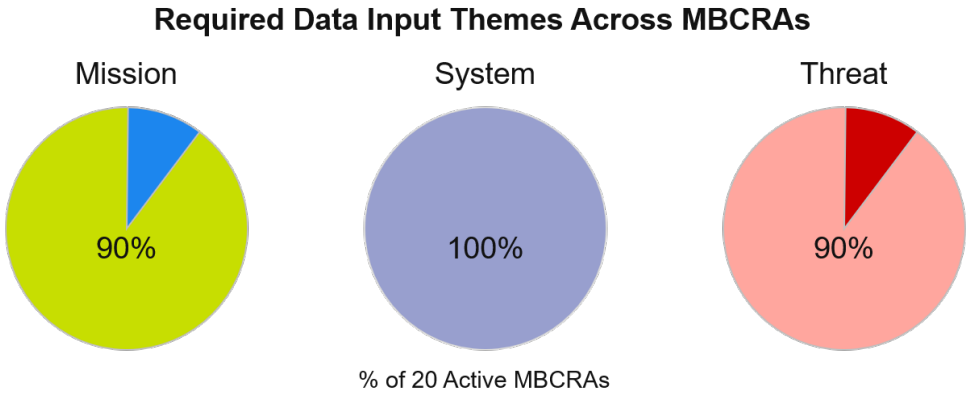

Figure 3. Common themes of required input data across the 20 active MBCRAs.

Summary of MBCRAs by required data input: Figure 4 shows the number of active MBCRAs for each of the 11 common required data inputs, grouped by theme. Seven of the required data inputs are shared by at least 50 percent (i.e., 10 out of 20) MBCRAs. System Architecture is the most shared data input, required by 90 percent (i.e., 18 out of 20) of the MBCRAs. The required data input with the lowest count is the Mitigations with only 25 percent (i.e., 5 out of 20) of the MBCRAs.

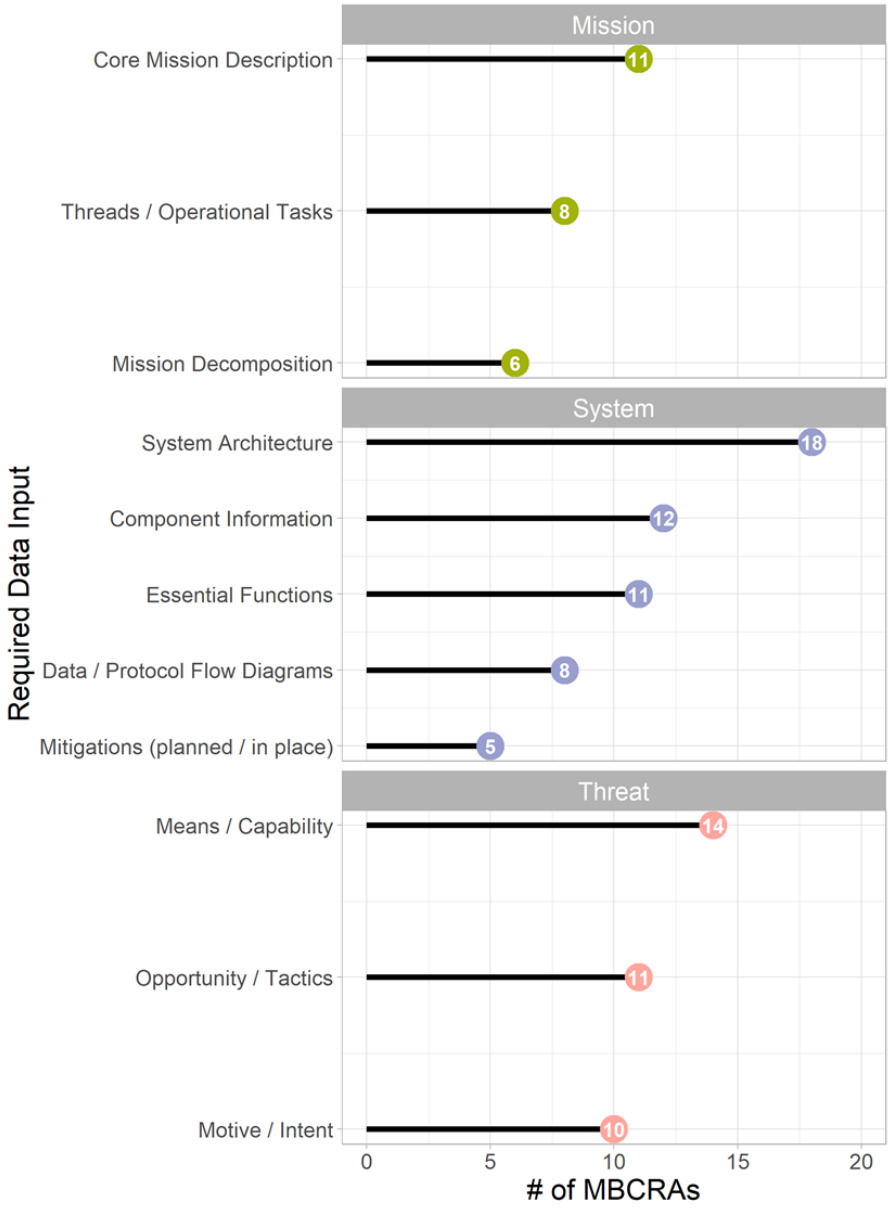

Figure 4. Common required data inputs across the 20 active MBCRAs.

Input information shared by several of the MBCRAs that did not meet our condition for "common required input data", included: impact or severity of adverse effect to the system, system vulnerabilities, test data or prior assessments, and timing of the mission. We think it is worth evaluating these additional shared information inputs in the context of developing metrics to assess the quality of the methodologies.

C. Formats for Data Output

IDA previously categorized the outputs for *all* the MBCRAs into five common output formats; we decided to keep this designation because all but one of the active MBCRAs use one of these formats to report results. No other output format was shared between the methodologies.[8] The *Mission Separable* category (with one methodology in use) does not report risk results in any of the common output formats. Figure 5 shows the number of active MBCRAs employing each of the six output formats for reporting results. Risk matrices or heat maps were used by the greatest number of active MBCRAs (13 out of 20) while Threat Scenarios were used by the fewest methodologies (3 out of 20).

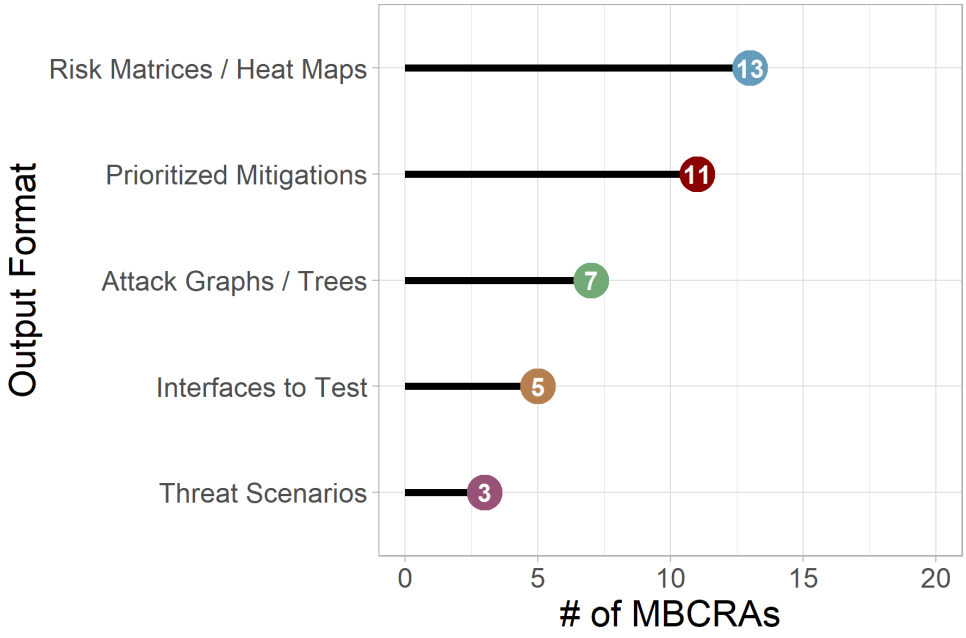

Figure 5. Common output formats for representing results across the 20 active MBCRAs.

D. MBCRA Information Flow

We paired the common data inputs and output formats in Figures 4 & 5 with the descriptive MBCRA categories to illustrate the connections across the 20 active MBCRAs in Figure 6. The line widths or links represent the number of methodologies between each of the three nodes: category, data inputs, and output format. Each of the 11 required data inputs map to at least one of the five outputs for the 20 active MBCRAs.

[8] MBCRAs can use multiple output formats to represent the results of the risk assessment.

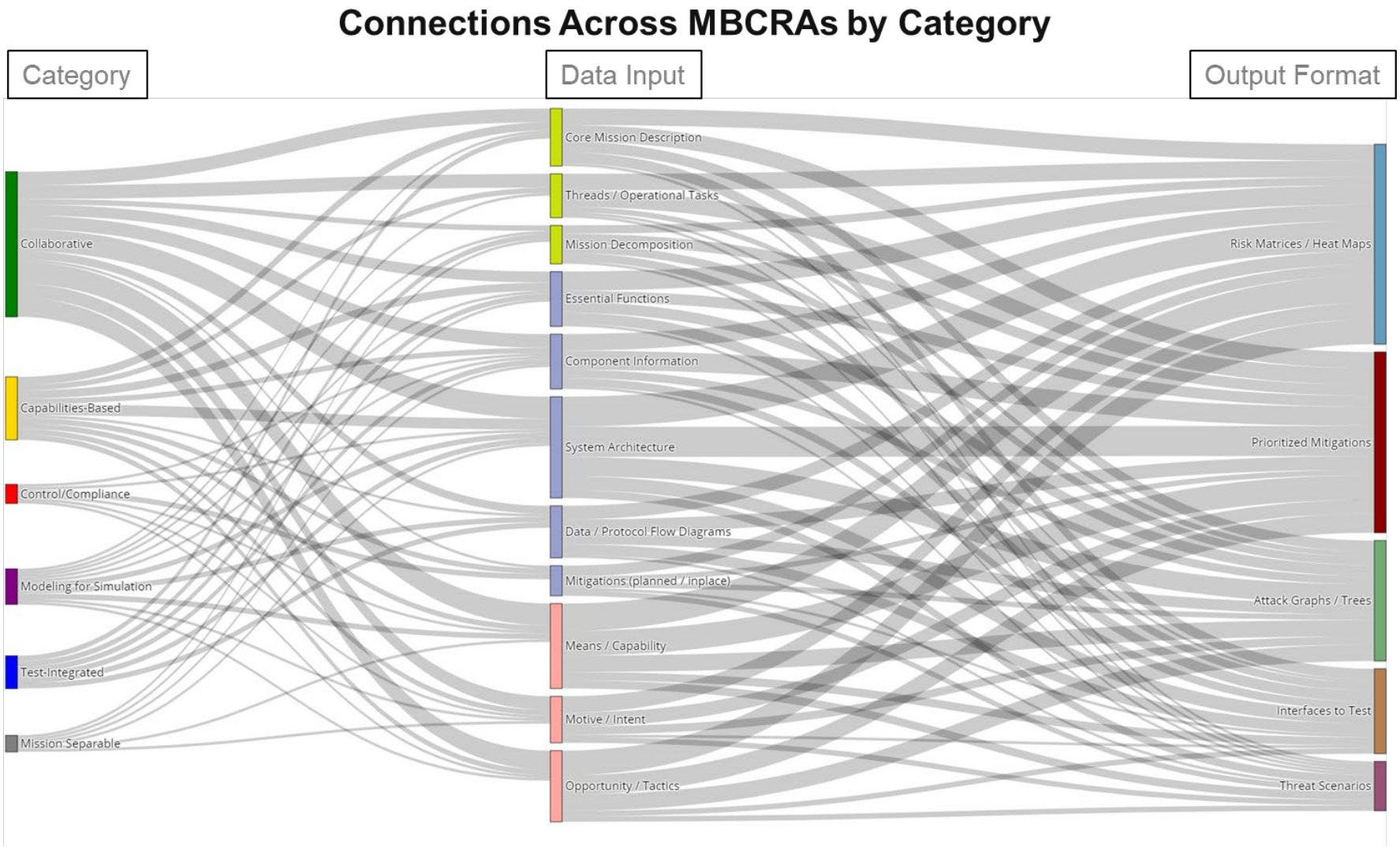

Figure 6. Diagram of the connections across inputs to outputs, by descriptive category, in the 20 active MBCRAs.

(This page is intentionally left blank.)

3. Conclusions

MBCRAs are an important tool in planning and testing for cybersecurity design throughout a system's developmental life cycle to ensure developing systems stay ahead of the evolving cyber threat. The test community continues to develop new methodologies without guidance or consensus on the characteristics of a quality type of analysis or criteria to assess system risk. As a first step toward building consensus, we document the commonalities between the MBCRAs currently in use, including: descriptive category; originating organization type; input information (organized by theme); and output formats. This analysis describes trends in "how" the MBCRAs known to be available to the DoD community are executed (in terms of inputs and outputs). Still missing are the answers to the "why" and "what" questions: why users select a specific MBCRA, what methodologies are actually used, and most importantly, what data or output result of an MBCRA are most valuable. Answers to these questions from users and stakeholders could better inform policy about MBCRAs.

Based on this analysis, IDA recommends the Office of the Director of Developmental Test, Evaluation, and Assessments consider the following when revising guidance on MBCRAs:

- The MBCRA descriptive categories offer a way to distinguish methodologies at a high-level but should not be used to evaluate their quality.
- Methodologies should include analysis of the mission, system and threat to be classified as MBCRAs.
- Analysis of the common input information across methodologies compared to the acquisition life cycle time frame could help inform MBCRA policy.
- MBCRA outputs (e.g., types of risk representation) that are most valuable and inform better designs should be evaluated when defining criteria.

(This page is intentionally left blank.)

Appendix A.
Abbreviations

DoD	Department of Defense
DoDI	Department of Defense Instruction
FFRDCs	Federally Funded Research and Development Centers
IDA	Institute for Defense Analyses
MBCRA	Mission Based Cyber Risk Assessment
UARCs	University Affiliated Research Centers

(This page is intentionally left blank.)

Appendix B.
References

Ambroso, Michael and Rhiannon Hutton, Comparative Review of DoD Mission-Based Cyber Risk Assessments, Alexandria, VA: Institute for Defense Analyses, P-8736, February 2018.

Department of Defense Instruction (DoDI) 5000.89 "Test and Evaluation", November 19, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF

de Naray, Rachel K. and Keith Galvin, Comparative Review of DoD MBCRAs: 2020 Updates and New Methodologies, Alexandria, VA: Institute for Defense Analyses, P-14309, September 2020.

(This page is intentionally left blank)

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
03-2022	IDA Paper	START DATE	END DATE Mar 2022

4. TITLE AND SUBTITLE
A Cross-Reference of Mission-Based Cyber Risk Assessment (MBCRA) Inputs and Outputs

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
HQ0034-19-D-0001		
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
AX-1-3100		

6. AUTHOR(S)
Buytendyk, Allyson, M.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305	P-32941 H 2022-000010

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER
Ms. Sarah Standard Cybersecurity/Interoperability Technical Director Director, Developmental Test, Evaluation and Assessments (D,DTE&A), OUSD R&E		

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Mission based cyber risk assessments (MBCRAs) are methodologies used to identify, estimate, assess and prioritize cybersecurity risks for hardware and information systems being employed in operations. Current Department of Defense (DoD) policy does not provide any guidance on how to evaluate the quality of mission-based cyber risk assessment methodologies; nor does it define specific criteria to examine or results that must be generated by MBCRAs to inform system security decisions. Using previous Institute for Defense Analyses (IDA) work in consultation with MBCRA source documentation in this study facilitated the development of a reference of common MBCRA data inputs and output formats, across the active methodologies. For the sample of twenty active MBCRAs identified there are eleven common required data inputs, five common output formats to report risk results and each data input maps to at least one of the risk reporting output formats. This analysis of the commonalities and connections between MBCRAs provides the DoD community information to inform evaluation criteria for MBCRA methodologies to support testing.

15. SUBJECT TERMS
Cyber; Cybersecurity; MBCRA; Mission context; Mission-Based; Risk; Risk Assessment; Test and Evaluation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	c. THIS PAGE		
Unclassified	Unclassified	Unclassified	SAR	

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER
John Hong	703-845-2564