INSTITUTE FOR DEFENSE ANALYSES

Analysis of Mission Based Cyber Risk Assessments (MBCRAs) Usage in DoD's Cyber Test & Evaluation

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

June 2022
IDA Publication P-33109
Log: H 2022-000221

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 HQ0034-19-D-0001, Project AX-1-3100, "Technical Analysis for the Director, Developmental Test, Evaluation, and Assessments," 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.

Distribution A: Cleared for public release by the DoD Office of Prepublication and Security Review, Case 22-S-2752, 1 September 2022

Acknowledgments

The authors would like to thank IDA committee, Dr. Stephen Ouellette (chair), Dr. Matthew R. Girardi, Dr. Davy Y. Lo, and Dr. Dr. Steven M. Nunes for providing technical review of this effort.

For More Information

Rachel Kuzio de Naray, Project Leader
rdenaray@ida.org, (703) 933-6556

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-33109

Analysis of Mission-Based Cyber Risk Assessment (MBCRA) Usage in DoD's Cyber Test & Evaluation

Rachel Kuzio de Naray (Project Leader)

Allyson M. Buytendyk (Principal Author)

Executive Summary

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

The Institute for Defense Analyses (IDA) therefore developed a short anonymous online survey with questions targeted at those who conduct MBCRAs to better understand their needs and information gaps when using such methodologies. We distributed a request to participate in the survey via an email to stakeholders in the Army, Air Force, Marine Corps, Navy and Space Force cyber T&E community. We also asked the stakeholders to forward the request to others who had experience in their organization. The survey was available from April 6-30, 2022 and had 30 respondents.

This paper provides an analysis of the survey responses to improve the use of MBCRAs and to help inform the development of MBCRA evaluation criteria to support the cyber test community.

Findings

- Respondents are primarily using the DoD-developed Cyber Table Top (CTT) and Air Force-developed Mission-based Risk Assessment Process for Cyber (MRAP-C) methodologies; both methodologies are categorized as *Collaborative*.[1]
- Respondents most value *System Architecture*[2] as a data input, but indicated this piece of information is most difficult to obtain, citing many reasons.

[1] IDA previously developed six descriptive categories to highlight difference between MBCRA methodologies (Ambroso 2017). *Collaborative* methodologies bring together program, cyber, intelligence, and other subject matter experts in a team-based risk assessment exercise.

[2] *System architecture* refers to diagrams or documentation that show boundaries and connections (e.g., interfaces, nodes, etc.) between artifacts in the system or sub-system.

- Of the 11 common MBCRA data inputs, *Incomplete documentation* or *inconsistent data* was/were cited as an issue by respondents.
- The MBCRA results deemed important by respondents, *Evaluate risk associated with vulnerabilities* and *Informs test design*, are consistent with the DoDI 5000.89 policy that directs program managers to 'identify those elements and interfaces of the system that, based on criticality and vulnerability analysis, need specific attention in T&E events.'
- Respondents indicated the main reason for selecting an MBCRA methodology was at the *Request of the stakeholders/program.*
- *Threat Scenarios*[3] were identified as the most important data output format by the respondents, with the reasons given as a *Communication tool for stakeholders* and to *Illustrate results in an easy to understand manner*. It is unclear if stakeholders also find this output format to be the most useful.
- *Potential Vulnerabilities Identified* and *Test Recommendations* are identified by the respondents as the most important MBCRA results. Evidence for how effective these findings are in the overall development of a system is still missing.

Recommendations

- Verify methodologies are consistent with DoDI 5000.89 and use appropriate criteria developed to evaluate MBCRAs (e.g., must include mission, system and threat information).
- Consider development of *Threat Scenarios* as a data output format or product of an MBCRA as an evaluation criteria of the methodology.
- Consult with program offices to better understand the rationale for selecting specific MBCRA methodologies over others and preference of output format when reviewing MBCRA results.
- Evaluate programs that have conducted MBCRAs to determine the thoroughness and rigor of the methodology (e.g., process includes active participation) and to develop measures of performance (e.g., number of vulnerabilities previously identified that are found in later test events) to quantify the return on investment for MBCRAs.

[3] *Threat Scenarios* are specific threats or conditions associated with the impact or consequence to the system in that circumstance.

- For programs that conduct MBCRAs with information constraints, assess which of the common data inputs may impact the quality of the results generated in the MBCRA with the specific methodology.

(This page is intentionally left blank.)

Contents

Tables

Figures

1. Introduction

Mission-based cyber risk assessments (MBCRAs) are methodologies used to identify, assess and prioritize cybersecurity risks[4] for hardware and information systems being employed in operations. Department of Defense Instruction (DoDI) 5000.89 "Test and Evaluation" (T&E) requires acquisition programs to conduct MBCRAs throughout a system's developmental life cycle to ensure that planning and testing for cybersecurity measures takes real-world context and mission impact into consideration. Current Department of Defense (DoD) policy, however, lacks guidance on how to evaluate the quality of MBCRAs developed by or for DoD to inform system security decisions.

As part of an on-going effort to inform evaluation criteria for MBCRA methodologies, in 2022 the Institute for Defense Analyses (IDA) documented the commonalities between 20 active[5] DoD MBCRA methodologies and developed a cross-reference of common data inputs[6] and output formats of the results (de Naray 2022). As a continuation of this effort, the current work identifies which MBCRA methodologies the cyber T&E community typically uses, why users select a specific MBCRA, what data inputs are most difficult to obtain, and what data output formats and overall result of an MBCRA are most valuable.

To gain insight, we developed a short, anonymous, online survey with questions targeted at those who conduct MBCRAs to better understand their needs and information gaps when using such methodologies. We distributed a request to participate in the survey via an email to stakeholders in the Army, Air Force, Marine Corps, Navy and Space Force cyber T&E community. We also asked the stakeholders to forward the request on to others who had experience in their organization. The survey was available from April 6-30, 2022 and had 30 respondents. Many of the respondents identified themselves as testers or

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

[5] de Naray 2022 defines an active MBCRA as a current methodology or the most recent version available.

[6] de Naray 2022 defines 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.

analysts working as contractors for the government. With the exception of the Army, all services were identified as the employer for at least one respondent.[7]

This paper provides an analysis of the survey results[8] collected from a targeted T&E audience to inform the development of criteria to evaluate the methodologies and results generated by MBCRAs.

[7] The intent of the question was to identify responses by service organization, but the wording of the question may have inadvertently caused those who support the Army (or other service) as a contractor to be miscategorized (Question 23 in Appendix C).

[8] See Appendix C for survey results discussed in this paper. Several additional survey questions were asked for other purposes but for brevity, are not included or discussed here.

2. Survey Insights

A. Use of MBCRA Methodologies

We asked survey respondents about their participation or involvement with MBCRAs and the specific methodologies they used (Questions 2, 4, and 7 in Appendix C). Both the mean (average) and the median number of MBCRA methodologies that respondents have had experience with (participated in or conducted) was three. MRAP-C and CTT had the most responses for both *Received training for* as well as *Most recent participation in the last five years* (Questions 4 & 7 in Appendix C). There were four write-in responses not included[9] in the survey list of active MBCRAs: Controls Attacks and Kinetic Effects Attacks (CAKE), System Theoretical Process Analysis (STPA) for Security, National Institute for Technology Special Publication 800-30 (NIST SP 800-30) and Functional Mission Analysis-Cyber (FMA-C). Figure 2-1 summarizes the survey respondents' use of specific MBCRAs and the associated descriptive category for each methodology.

[9] IDA's 2017 and 2020 comparative reviews of DoD MBCRAs (Ambroso 2017, de Naray 2020) were the primary sources used to define the list of 20 active MBCRAs for the survey.

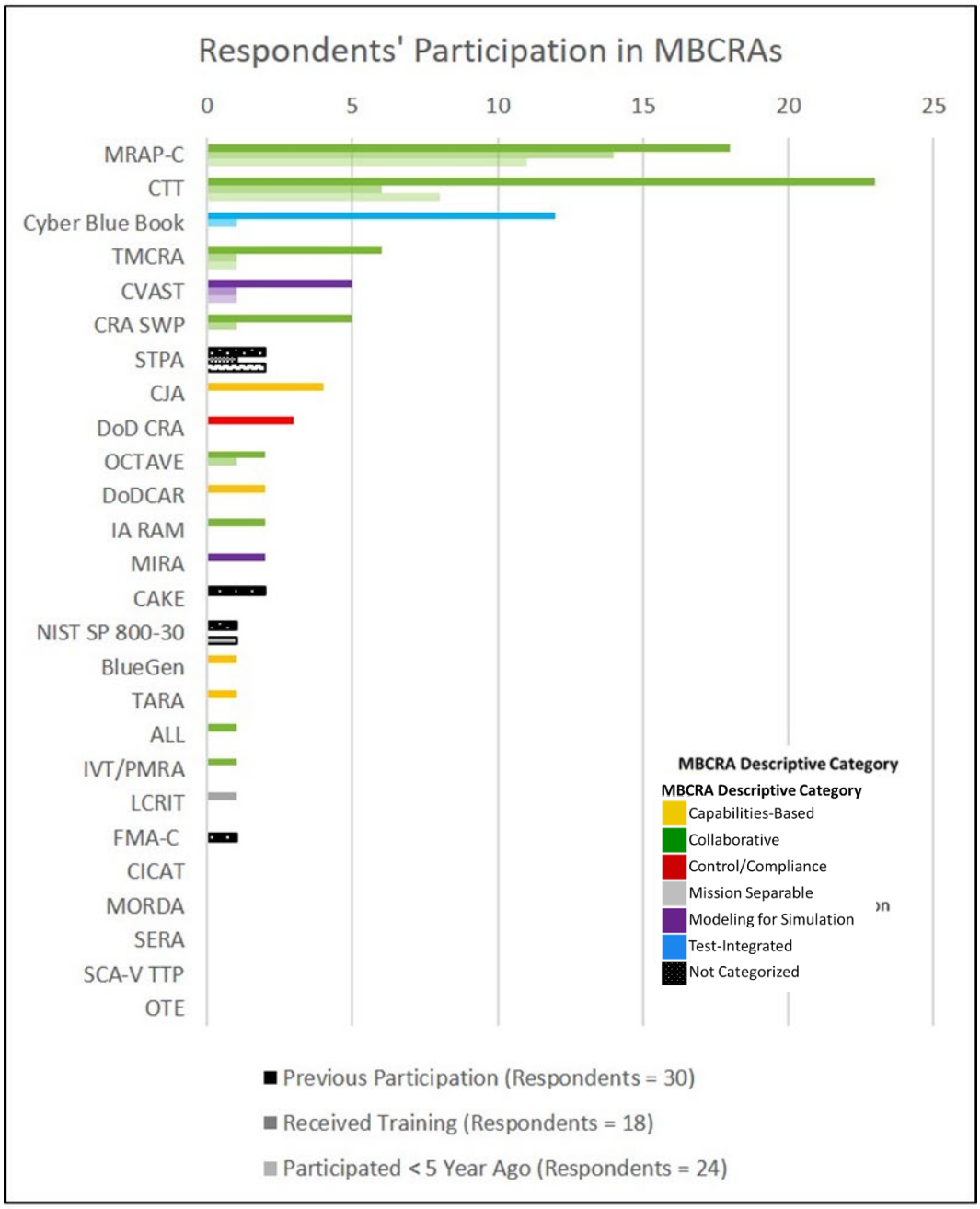


Figure 2-1. Survey respondents' participation in various MBCRA methodologies

As shown in Figure 2-1, respondents primarily participated in *Collaborative*[10] type methodologies, particularly the Air Force-developed MRAP-C process and the DoD-developed CTT process. This is consistent with IDA's observation of the increase in development of *Collaborative* type MBCRAs, indicating the cyber T&E community's preference for this type of methodology (de Naray 2022).[11]

The previous IDA comparative reviews[12] of DoD MBCRAs were not exhaustive, so respondents were able to write in other methodologies they have used. One response that stood out was NIST SP 800-30, which defines a general approach to risk assessment and the framework for many MBCRA methodologies. It is unclear whether following the general approach described in NIST SP 800-30 adequately satisfies DoDI 5000.89 policy for conducting an MBCRA. This exemplifies the need for clear criteria to evaluate what constitutes an acceptable MBCRA. If evaluation criteria for MBCRAs were established, DoD could use them to verify and endorse that the methodology chosen by a program satisfactorily 'identifies those elements and interfaces of the system that, based on criticality and vulnerability analysis, need specific attention in T&E events' as outlined in DoDI 5000.89.

B. Reasons for MBCRA Methodology Selection

We asked those survey respondents who indicated they were involved in an MBCRA less than five years ago to explain the reason for the selection of that methodology over another (Question 8 in Appendix C). We reviewed the 26 written responses and binned them into five groups. The majority (5 out of 8) of responses for selecting a CTT was at the *Request of the stakeholders/program*. The reasons why MRAP-C was selected were split between the *Request of the stakeholders/program* and *Methodology fit the need*. Figure 2-2 summarizes all the survey responses about selecting CTT or MRAP-C across the five groups.[13]

---

[10] IDA previously developed six descriptive categories: *Capabilities-Based*, *Collaborative*, *Control/Compliance*, *Mission Separable*, *Modeling for Simulation* and *Test-Integrated*, to highlight difference between MBCRA methodologies (Ambroso 2017).

[11] Between 2017 and 2020 the distribution of total active MBCRA methodologies across descriptive categories shifted from close to a third to about half categorized as *Collaborative* (de Naray 2022).

[12] Ambroso 2017; de Naray 2020.

[13] There was a total of six MBCRAs out of the 26 responses; 19 indicated either MRAP-C or CTT (Question 7 in Appendix C).

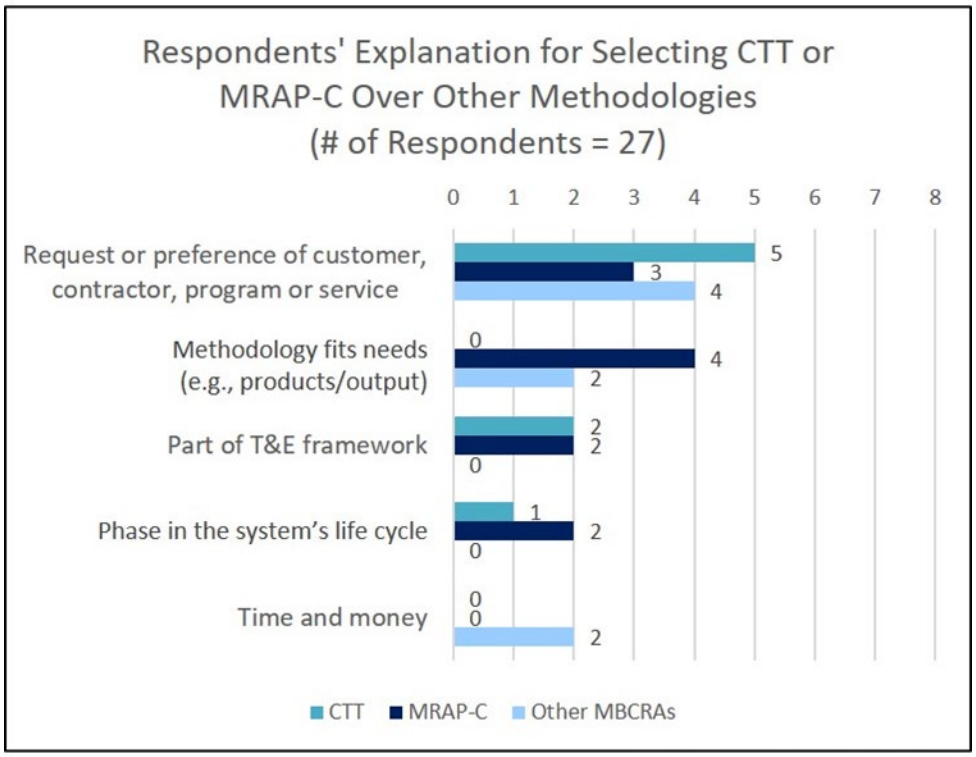


Figure 2-2. Survey respondents' reasons for selection of CTT or MRAP-C over other MBCRAs

One notable observation about the survey responses for those that recently participated in a CTT or MRAP-C is that no one indicated *Time and money* as a reason for selecting those methodologies. Almost half of the responses on reasons for MBCRA methodology selection indicated that those participating in an event were not involved in the methodology selection process. The target audience of the survey was the test community, specifically cyber subject matter experts, who may not have had insight into the decisions behind selecting an MBCRA methodology. For future surveys, the question about MBCRA choice should be directed to the program office to better understand the rationale for their selection.

C. Obtaining Required Input Data to MBCRA Methodologies

We asked survey respondents to indicate which of the 11 common data inputs previously identified[14] were difficult to obtain for an MBCRA and to explain their reasons (Questions 15 and 16 in Appendix C). We categorized the respondents' reasons into seven groups and mapped them to each data input indicated. Next, we tabulated a difficulty score based on the number of responses (see Table 2-1).

[14] See de Naray 2022 for more information about the common data inputs to MBCRA methodologies.

Table 2-1. Ranking of survey responses to indicate difficulty obtaining MBCRA input data

# of Responses	Difficulty Ranking
30-26	Very Difficult
25-21	Hard
20-16	Medium Challenge
<15	Manageable

Then, we assigned an impact score based on the number of MBCRA methodologies that required each data input[15] (see Table 2-2). This assumed equal weighting of the 20 different methodologies.

Table 2-2. Ranking of MBCRA methodologies that require specific piece of input data

# of Methodologies	Impact Ranking
20-16	Most
15-11	Many
10-6	Several
<5	Few

[15] Data inputs were mapped to methodologies in de Naray 2022.

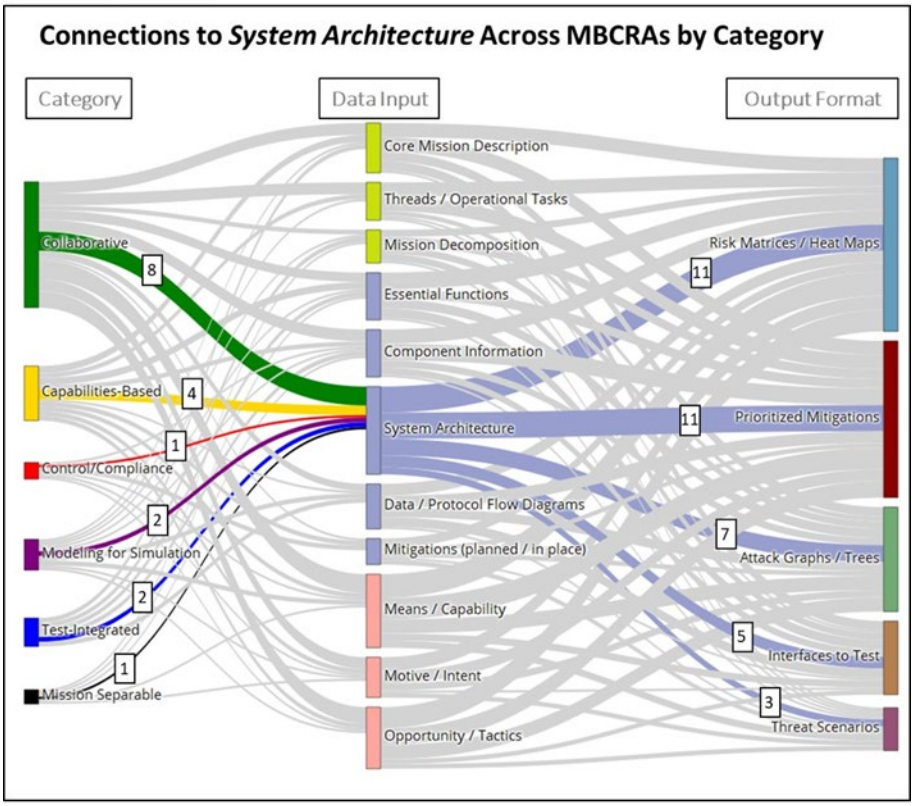
Table 2-3 summarizes the respondents' reasons for why data input is difficult to obtain and provides the difficulty and impact rankings for each category of data input. Cells in the top portion of the table are colored green, blue or pink if at least one response related to data input was provided. There is difficulty obtaining information across the general "Threat" category of data inputs (pink): 15 of 21 (71 percent) of the data inputs have reasons cited for why it is hard. The respondents indicated difficulty obtaining "System" information (blue) for 23 of 35 (66 percent) of the data inputs, and for 7 of 21 (33 percent) of the "Mission" data inputs (green). The *System Architecture*[16] is the only data input that scored 'Very Difficult' to obtain and is required by 'Most' MBCRA methodologies (both cells at the bottom of the column are red). There were five reasons cited as to why *System Architecture* information or data are difficult to get, indicating this is a complex problem.

Table 2-3. Summary of survey respondents' reasons for difficulty in obtaining specific MBCRA data inputs

	Mission			System					Threat		
Respondents' Reasons Data Inputs are Difficult to Obtain	Mission Decomposition	Core Mission Description	Threads / Operational Tasks	Data/Protocol Flow Diagrams	Essential Functions	System Architecture	Component Information	Mitigations	Opportunity / Tactics	Means / Capability	Motive / Intent
Insufficient level of detail in intelligence data											
Incomplete documentation, inaccurate/inconsistent data											
Access to classified information due to personnel's security clearance											
Identifying personnel who have the required data and knowledge about it											
Information not defined in early development											
Access to scope of operational missions											
Time to receive information											
Difficulty Obtaining Information (n=30)	28	27	24	29	29	29	25	16	29	28	21
MBCRA Methodologies Impacted (n=20)	6	11	8	8	11	18	12	5	11	14	10

[16] *System architecture* refers to diagrams or documentation that show boundaries and connections (e.g., interfaces, nodes, etc.) between artifacts in the system or sub-system.

Next, we identified which MBCRA methodologies required *System Architecture* data to determine the types of output formats that would be affected by insufficient information. To do this, we used the connections between methodologies, organized by descriptive category, found across the 20 active MBCRAs methodologies in the previous IDA study (de Naray 2022). In Figure 2-3, if at least one MBCRA methodology in a descriptive category requires *System Architecture* input data, a colored link connects the category node on the left side to the light blue *System Architecture* node in the middle. Blue links from *System Architecture* to output format nodes on the right indicate that *System Architecture* information is required to generate that type of output format. As seen in the figure, all categories of output format rely on *System Architecture* information. This further illustrates the importance of *System Architecture* information in conducting any MBCRA. Additionally, since *System Architecture* is not the only common data input category to score as "Very Difficult" (7 of the 11 categories had this ranking), it is likely that most MBCRAs are conducted with constraints on input information and corresponding limitations on output.



Line widths or links represent the number of methodologies between each node. Number shown is the number of MBCRAs that require System Architecture as a data input and inform which types of data output formats.

Figure 2-3. Diagram of connections across inputs to outputs, by descriptive category, in the 20 active MBCRAs.

Respondents reported *Incomplete documentation or inconsistent data* as a source of difficulty in obtaining data information across all common MBCRA inputs. Insufficient or unobtainable data inputs when conducting an MBCRA likely affects the quality of the data outputs and could lead to misleading results. An assessment of programs that conducted MBCRAs with information constraints would provide insight into what the consequences are and which data inputs are most critical to the process.

D. Value of Common Output Formats in MBCRA Methodologies

We also asked survey respondents to indicate which of the five common data output formats previously identified[17] for MBCRAs they value or view as important and to explain their reasons (Questions 19 and 20 in Appendix C). We categorized the respondents' reasons "why" into four groups and mapped them to each data output format indicated by the respondent. Next, we assigned an importance score based on the number of responses (using the same number of responses to score the input data difficulty) for each data output format as shown in Table 2-4.

Table 2-4. Ranking of survey responses to indicate importance/value of MBCRA information

# of Responses	Importance Ranking
30-26	Necessary
25-21	Important
20-16	Nice to Have
<15	Ok

Then, we assigned an impact score (using the same number of methodologies to score the required input data) based on the number of MBCRA methodologies that generate each type of data output format in their process as shown in Table 2-5 (de Naray 2022).

[17] See de Naray 2022 for more information about the common data output formats from MBCRA methodologies.

Table 2-5. Ranking of MBCRA methodologies that generate specific data output formats

# of Methodologies	Impact Ranking
20-16	Most
15-11	Many
10-6	Several
<5	Few

The respondents' reasons for valuing each data output format are summarized in Table 2-6; the scores showing the importance to and impact on the methodologies are also included. As shown in the table, the *Threat Scenarios* output format scored 'Important' (i.e., 21 positive responses) yet these are generated by only a 'Few' (i.e., three) MBCRA methodologies; there is a clear gap in the data output format valued by the respondents and what most of the MBCRA methodologies produce. The two methodologies most used by the survey respondents, CTT and MRAP-C, are two of the three methodologies that generate *Threat Scenarios* as a data output format.

Table 2-6. Summary of survey respondents' reasons for specific MBCRA data output format value

	Threat Scenarios	Risk Matrices/ Heat Maps	Prioritized Mitigations	Interfaces to Test	Attack Graphs/ Trees
Respondents' Reasons Why Valued (n=21) Top Responses (>4 responses)	Communication tool to inform stakeholders (e.g. program office, senior leadership) Illustrates results in a focused/easy to understand manner	Illustrates results in a focused/easy to understand manner	Communication tool to inform stakeholders (e.g. program office, senior leadership)	Informs future T&E objectives	
Importance of Output Format (n=30)	21	19	17	16	12
MBCRA Methodologies Impacted (n=20)	3	13	11	5	7
CTT Outputs	X	X		X	
MRAP-C Outputs	X	X	X	X	X

Respondents also shared the top reasons why Threat Scenarios are viewed as important, indicating that it is because they are a Communication tool for stakeholders and Illustrate results in an easy to understand manner. Earlier responses (see Figure 2-2) showed respondents had little insight into the decisions behind selecting an MBCRA methodology. There could be an inconsistency between stakeholders' preferred MBCRA methodology and MBCRA products (e.g., data output format for MBCRA results). The

question about the MBCRA data output format should be directed to the program office to better understand what communication tool for MBCRA results they value.

E. Value of Results from MBCRA Methodologies

We asked survey respondents to indicate which of the five types of information or results from MBCRAs they value and to explain their reasons (Questions 17 and 18 in Appendix C). We categorized the respondents' reasons "why" into four groups and mapped them to each result indicated by the respondent. Again, we assigned an importance score based on the number of responses for each MBCRA result (see Table 2-4).

Table 2-7 summarizes the respondents' reasons for each result accompanied by the importance scores as outlined in Table 2-4. Both *Potential Vulnerabilities Identified* and *Test Recommendations* scored 'Necessary' and respondents cited *Informs test design, strategy* and *Informs how to manage/prioritize cyber risk* as the top reasons.

Table 2-7. Summary of survey respondents' reasons for specific MBCRA results importance

	Potential Vulnerabilities Identified	Test Recommendations	Determination of Attack(s) Likelihood	Mitigations	Risk Depiction
Respondents' Reasons Why Important (n = 22) ***Primary Reasons*** (12-9 responses)	Informs test design, strategy			Informs how to manage/prioritize cyber risk	
	Informs how to manage/prioritize cyber risk				
Secondary Reasons (8-6 responses)	Informs engineering process, design decisions			Informs test design, strategy	
	Provides information to help understand the system in a real world conext , informs owners, opererators, developers			Informs engineering process, design decisions	
Importance of MBCRA Result (n=30)	26	26	24	20	19

We then compared the 'Necessary' MBCRA results and reasons with the responses given by respondents about the top objective(s) for the most recent MBCRA they participated in and an explanation for why the MBCRA results favorably met the objective(s) (Questions 9 and 11 Appendix C). The respondents' top reasons for the value of specific MBCRA results were very similar to the MBCRA objectives with the greatest number of responses (see Table 2-8). Also, about two thirds (12 out of 19 responses) of the reasons why respondents' most recent MBCRA favorably met the objectives of the event were very similar to the respondents' highest valued MBCRA results: *Potential Vulnerabilities Identified* and *Test Recommendations.*

Table 2-8. Summary of survey respondents' most recent MBCRA objective & results

Top Objectives of Most Recent MBCRA (n=27)	# of Responses	Top Reasons Why Most Recent MBCRA Met Objective (n=19)	# of Responses
Evaluate risk associated with previously identified vulnerabilities	21	Informed test design, strategy, events; TEMP	4
		Created attack paths/vectors	3
Inform test design	20	Identified possible vulnerabilities	3
		Informed AA or CVPA	2

We also asked respondents about the frequency with which MBCRA results inform a future MBCRA (Question 21 in Appendix C). About 48 percent responded that this occurs ''Frequently' or 'Very frequently' (see Figure 2-4). Similarly, we gathered responses about the adequacy of budgets to conduct MBCRAs (Question 22 in Appendix C). About 45 percent of respondents indicated 'Neutral' as their response to whether the MBCRA budget is sufficient to conduct an effective assessment (see Figure 2-5).

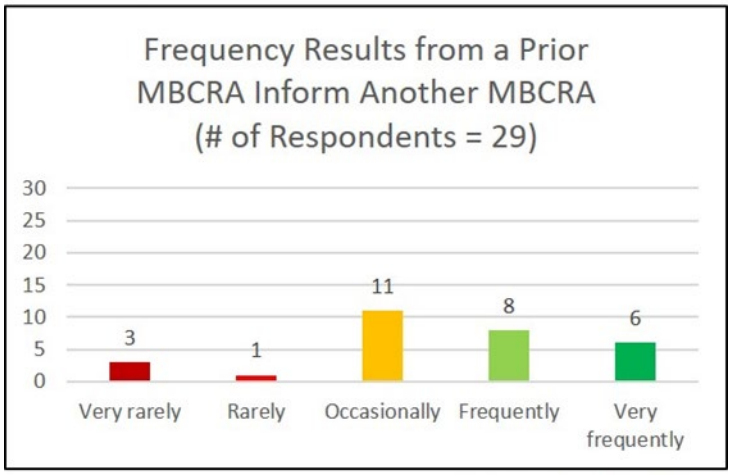


Figure 2-4. Survey responses about frequency MBCRA results inform future MBCRA events

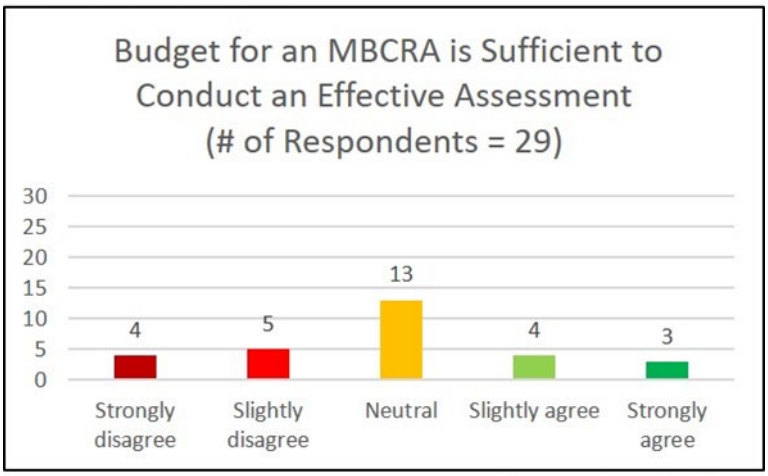


Figure 2-5. Survey responses about sufficiency of budgets to conduct effective MBCRAs

Survey responses show that MBCRA results valued by the respondents align with and generally meet the common MBCRA objectives. Responses did not provide a definitive indicator as to whether the money budgeted for an MBCRA is a factor in producing results. More importantly, it is unclear how effective results generated by MBCRAs are in the overall development of a system. An evaluation of programs that have done MBCRAs could measure their value and results, and quantify the return on investment.

3. Conclusions

MBCRAs are an important tool in planning and testing for cybersecurity design throughout a system's developmental life cycle to ensure the system in development stays ahead of the evolving cyber threat. As part of a larger effort to define criteria to evaluate MBCRA methodologies in generating results and informing cybersecurity testing, we conducted a short anonymous online survey targeted at the cyber T&E community and analyzed the responses. We sought answers about what methodologies are commonly used, why users select a specific MBCRA methodology over others, what data inputs are most difficult to obtain, and what data output formats and overall result of an MBCRA are most useful for informing cyber testing.

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

- Verify methodologies are consistent with DoDI 5000.89 and use appropriate criteria developed to evaluate MBCRAs (e.g., must include mission, system and threat information).
- Consider development of *Threat Scenarios* as a data output format or product of an MBCRA as an evaluation criteria of the methodology.
- Consult with program offices to better understand the rationale for selecting specific MBCRA methodologies over others and preference of output format when reviewing MBCRA results.
- Evaluate programs that have conducted MBCRAs to determine the thoroughness and rigor of the methodology (e.g., process includes active participation) and to develop measures of performance (e.g., number of vulnerabilities previously identified that are found in later test events) to quantify the return on investment for MBCRAs.
- For programs that conduct MBCRAs with information constraints, assess which of the common data inputs may impact the quality of the results generated in the MBCRA with the specific methodology.

(This page is intentionally left blank.)

Appendix A.
Abbreviations

AA	Adversarial Assessment
ALL	ACTWG Lessons Learned
CAKE	Controls Attacks and Kinetic Effects Attacks
CBB	Cyber Blue Book
CICAT	Critical Infrastructure Cyberspace Analysis Tool
CJA	Crown Jewels Assessment
CRA SWP	Cyber Risk Assessment Standard Work Package
CTT	Cyber Table Top
CVAST	Cyber Vulnerability Assessment Tool
CVPA	Cooperative Vulnerability and Penetration Assessment
DoD	Department of Defense
DoD CRA	DoD Cybersecurity Risk Assessment Guide
DoDCAR	DoD Cybersecurity Analysis and Review
DoDI	Department of Defense Instruction
FMA-C	Functional Mission Analysis-Cyber
IDA	Institute for Defense Analyses
IA RAM	Information Assurance Risk Assessment Methodology
IVT/PMRA	Impact, Vulnerability, and Threat / Probabilistic Mission Risk Analysis
LCRIT	Logistics Cyber Risk Identification Tool
MBCRA	Mission-Based Cyber Risk Assessment
MIRA	Mission Information Risk Analysis
MORDA	Mission Oriented Risk and Design Analysis
MRAP-C	Mission-based Risk Assessment Process for Cyber
NIST SP 800-30	National Institute for Technology Special Publication 800-30
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OTE	Cyber Operational Test and Evaluation Methodology
PPSM	Ports, Protocols, and Services Management

SCA-V TTP	Security Control Assessor – Validator Operational Tactics, Techniques, and Procedures
SERA	Security Engineering Risk Analysis
STPA	System Theoretical Process Analysis for Security
TARA	Threat Assessment and Remediation Analysis
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TMCRA	Tabletop Mission Cyber Risk Assessment
UARC	University Affiliated Research Center

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 Kuzio and Allyson Buytendyk. A Cross-Reference of Mission-Based Cyber Risk Assessment (MBCRA) Inputs and Outputs. Alexandria, VA: Institute for Defense Analyses, P-32941, March 2022.

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.)

Appendix C.
MBCRA Survey Questions and Responses

Questions about MBCRA Background:

1. How would you describe your knowledge of MBCRAs? (select one)

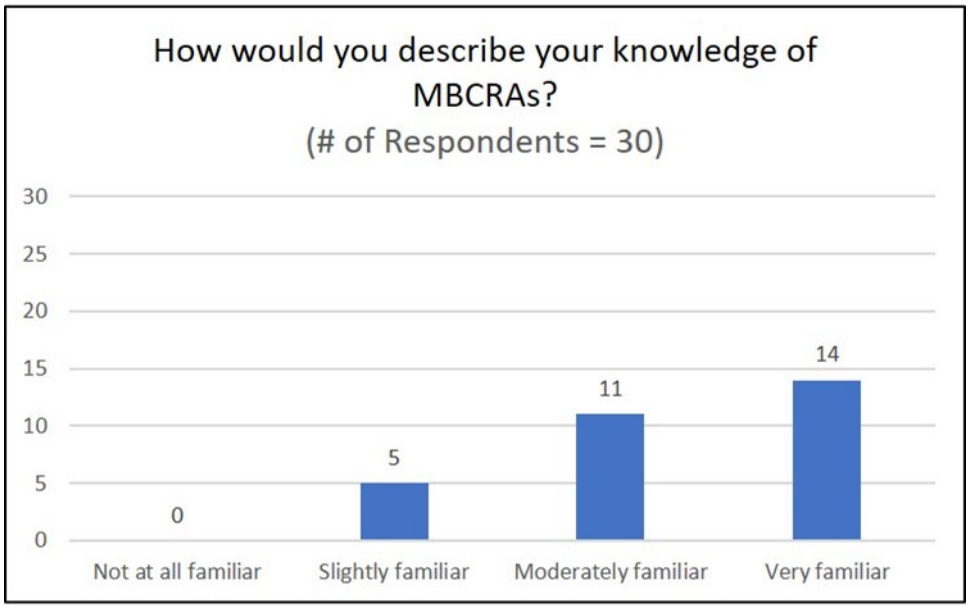


Figure C-1. Survey responses to Question 1

2. Which MBCRAs have you supported development of, participated in or conducted? (select all that apply)

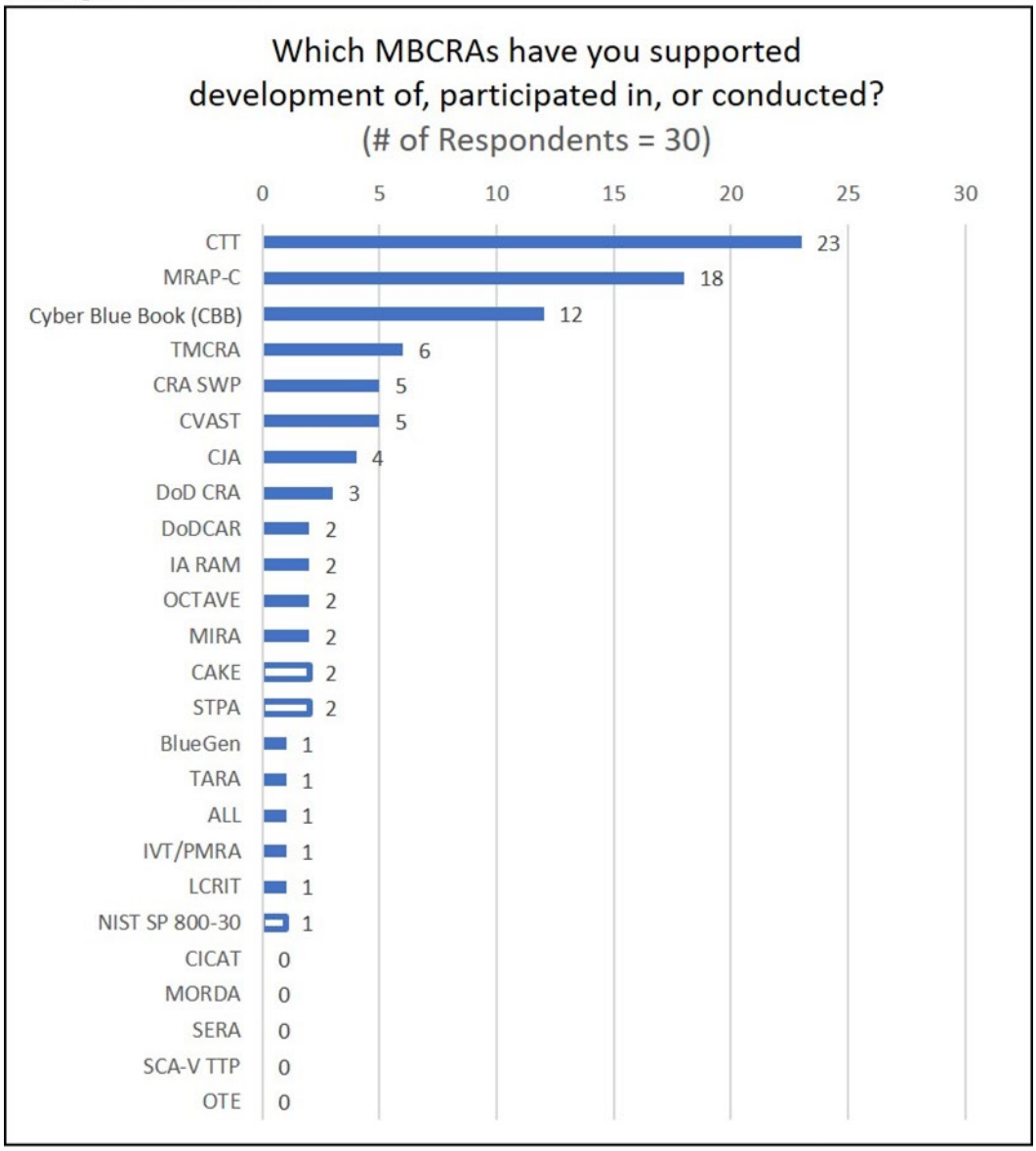


Figure C-2. Survey responses to Question 2. Empty bars indicate write-in responses provided when "Other" was selected.

3. Have you attended any training or class for a specific MBCRA? (select one)

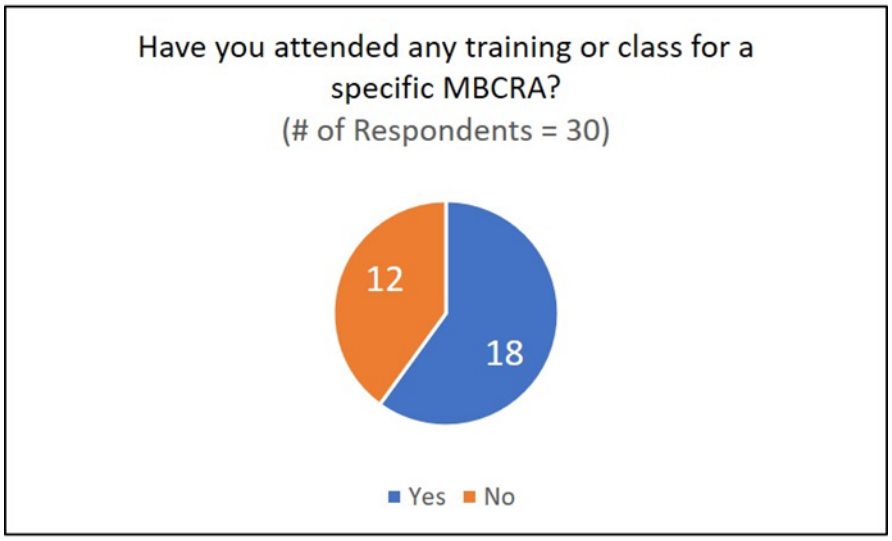


Figure C-3. Survey responses to Question 3

A response of not attending training for an MBCRA in Question 3 excluded those from answering Question 4.

4. Please list the MBCRA(s) you received training for: (write-in)

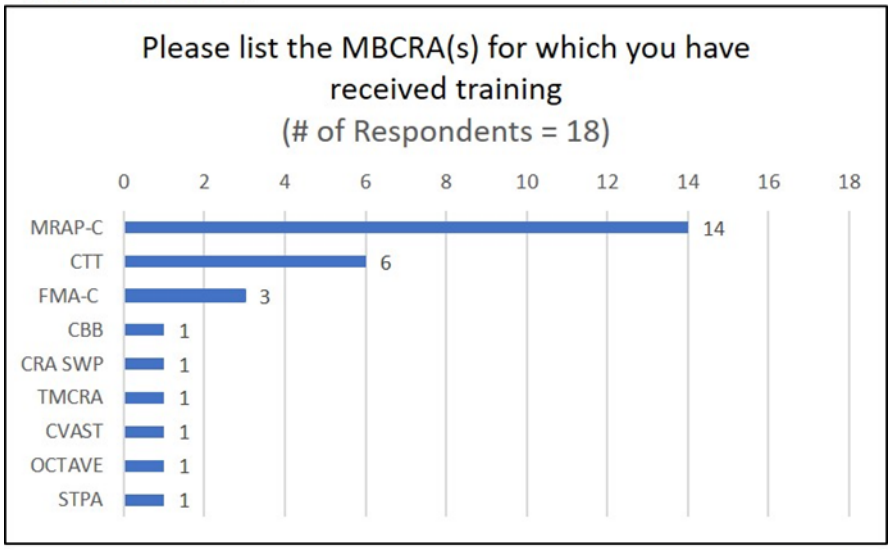


Figure C-4. Survey responses to Question 4

5. Approximately how many MBCRAs have you participated in or conducted? (select one)

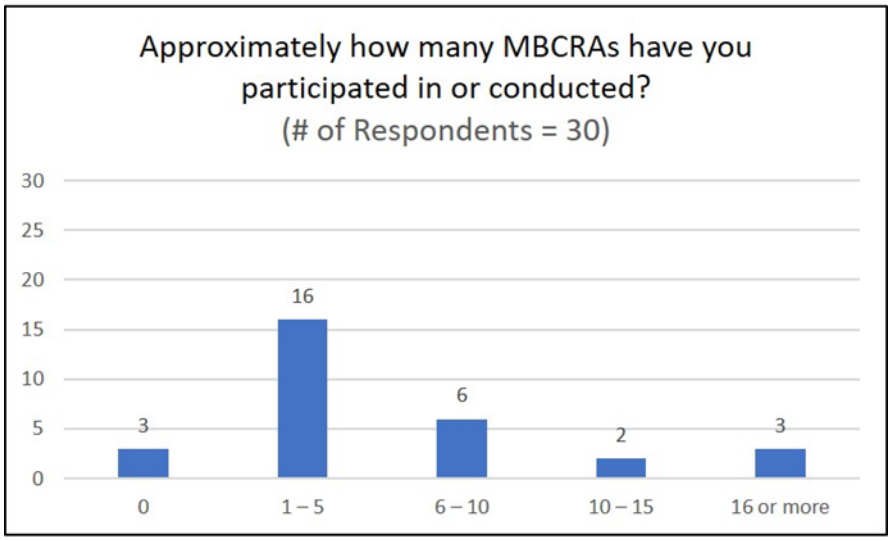


Figure C-5. Survey responses to Question 5

A response of participating in zero MBCRAs in Question 5 excluded those from answering Question 6.

6. When did you last participate in or conduct an MBCRA? (select one)

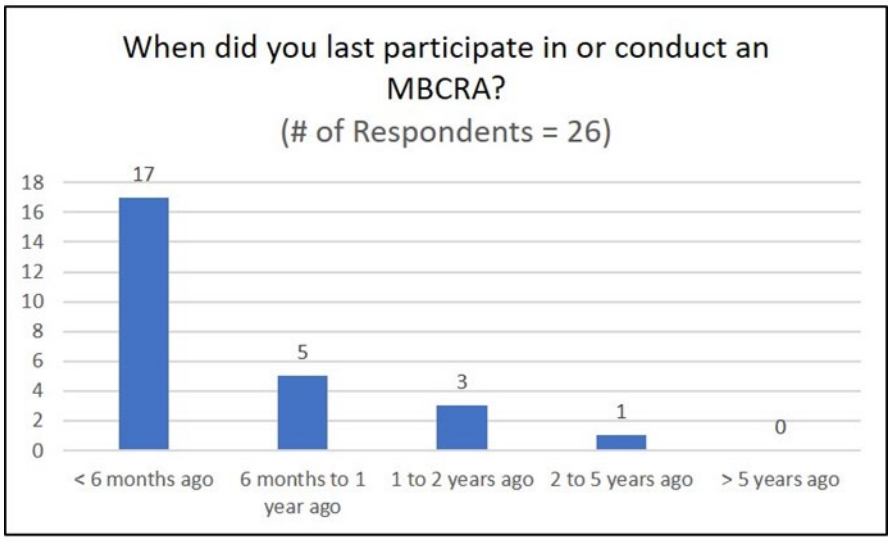


Figure C-6. Survey responses to Questions 6

Questions about the MBCRA Most Recently Participated in/Conducted

A response of participating in zero MBCRAs in Question 5 or participated in an MBCRA more than 5 years ago excluded those from answering Questions 7-11.

7. Which MBCRA did you most recently participate in or conduct? (write-in)

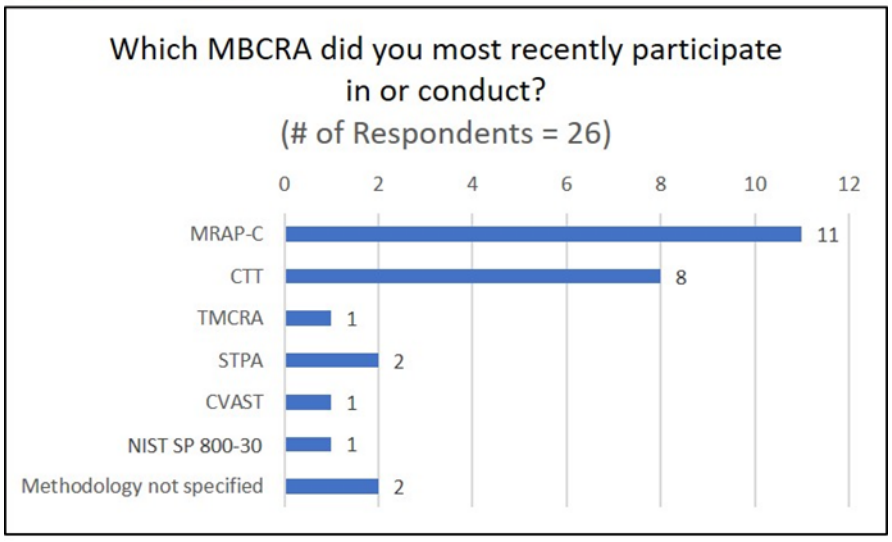


Figure C-7. Survey responses to Question 7

8. Why was that MBCRA selected over the other methodologies? (write-in)

Table C-1. Survey Responses to Question 8

Categorization of Written Responses	# of Responses*
Request/preference of customer, contractor, program or service	11
Methodology fits needs (e.g., products/output)	6
Part of T&E framework	4
Phase in the system's life cycle	3
Time and money	2

* Total respondents = 26.

9. What was (were) the objective(s) for the assessment? (select all that apply)

Table C-2. Survey responses to Question 9

Selected Responses	# of Responses*
Evaluate risk associated with previously identified vulnerabilities	21
Inform test design	20
Inform system design	12
Incorporate results from cooperative and/or adversarial test events	7
Evaluate cost/benefits of proposed mitigations	3
Run sensitivity study	0
Write-in Responses	
“Create mission templates”	8
“Inform RMF analysis/activities”	2
“Develop recommendation on identified potential vulnerabilities”	1
“Develop future cyber test objectives”	1
“Inform requirements and contract language”	1
“Support compliance of pen test”	1

* Total respondents = 27.

10. Did the results from the MBCRA meet the objective(s) for conducting the assessment?

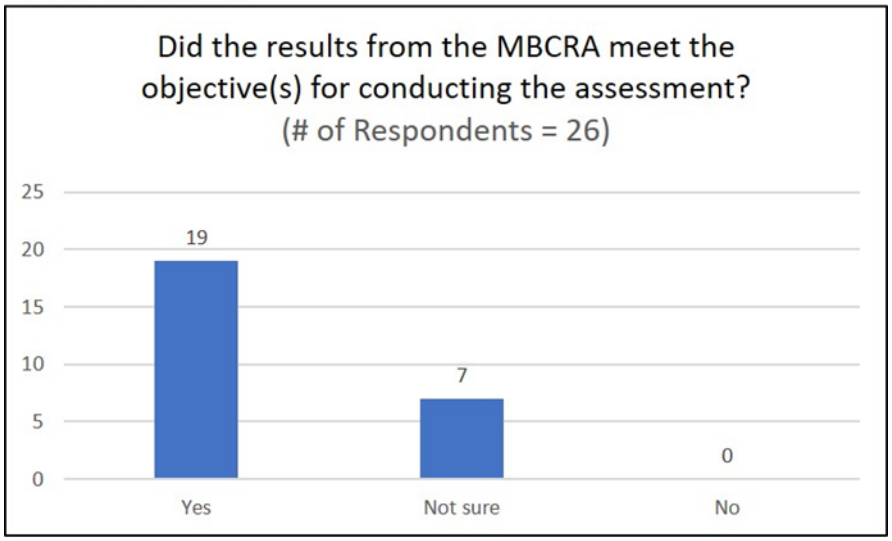


Figure C-8. Survey responses to Question 10

11. Please explain why the results from the MBCRA did or did not meet the objective(s) for conducting the assessment: (write-in)

Table C-3. Survey Responses to Question 11

Explanation for 'Yes' Responses in Question 10	# of Responses*
Informed test design, strategy, schedule, events; test & evaluation master plan (TEMP)	4
Identified possible vulnerabilities	3
Communicated risk	3
Created attack paths/vectors	3
Informed system design changes	2
Informed requirements	2
Educated contractors, engineers, program staff about vulnerabilities.	2
Informed Adversarial Assessment (AA) or Cooperative Vulnerability and Penetration Assessment (CVPA)	2
Provided a repeatable process	1
Early in the program	1
Explanation for 'No' Responses in Question 10	
Lack of visibility in objective or how results used (e.g., contractor led, limited insight about program)	3
Still working to finalize results	3
Contractor support not included in contract language	1
MBCRA results in agile development may be irrelevant with design changes	1

* Total respondents = 24.

Questions about MBCRA Data Inputs

12. What type of information or data inputs are needed prior to the MBCRA to develop a well-defined mission? (select all that apply)

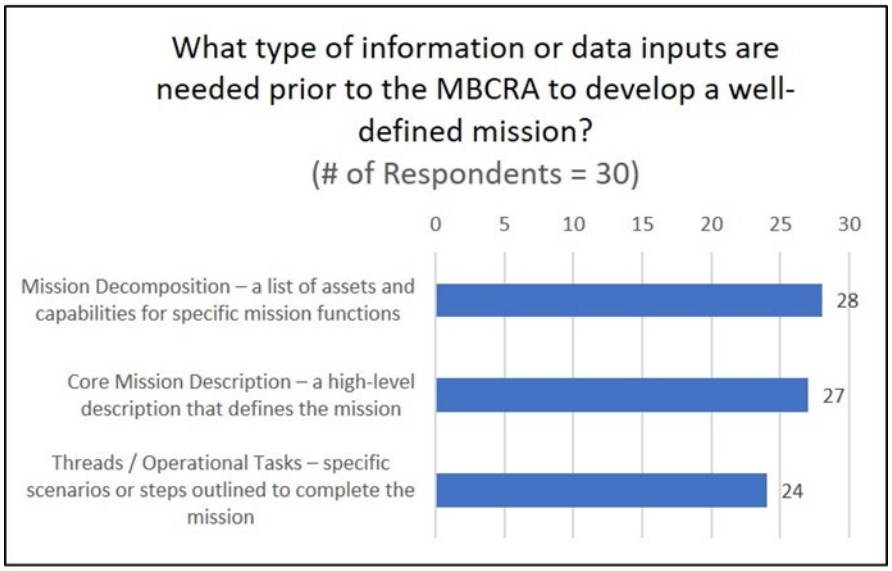


Figure C-9. Survey responses selected for Question 12

Table C-4. Survey responses written for Question 12

Write-in Responses	# of Responses
"Attack paths."	1
"Platforms, systems, and connective tissue that make up the targeted environment."	1
"Training/User guides for critical mission systems and components."	1
"System network/connectivity design concepts."	1

13. What type of information or data inputs are needed prior to the MBCRA to provide a high-fidelity system representation? (select all the apply)

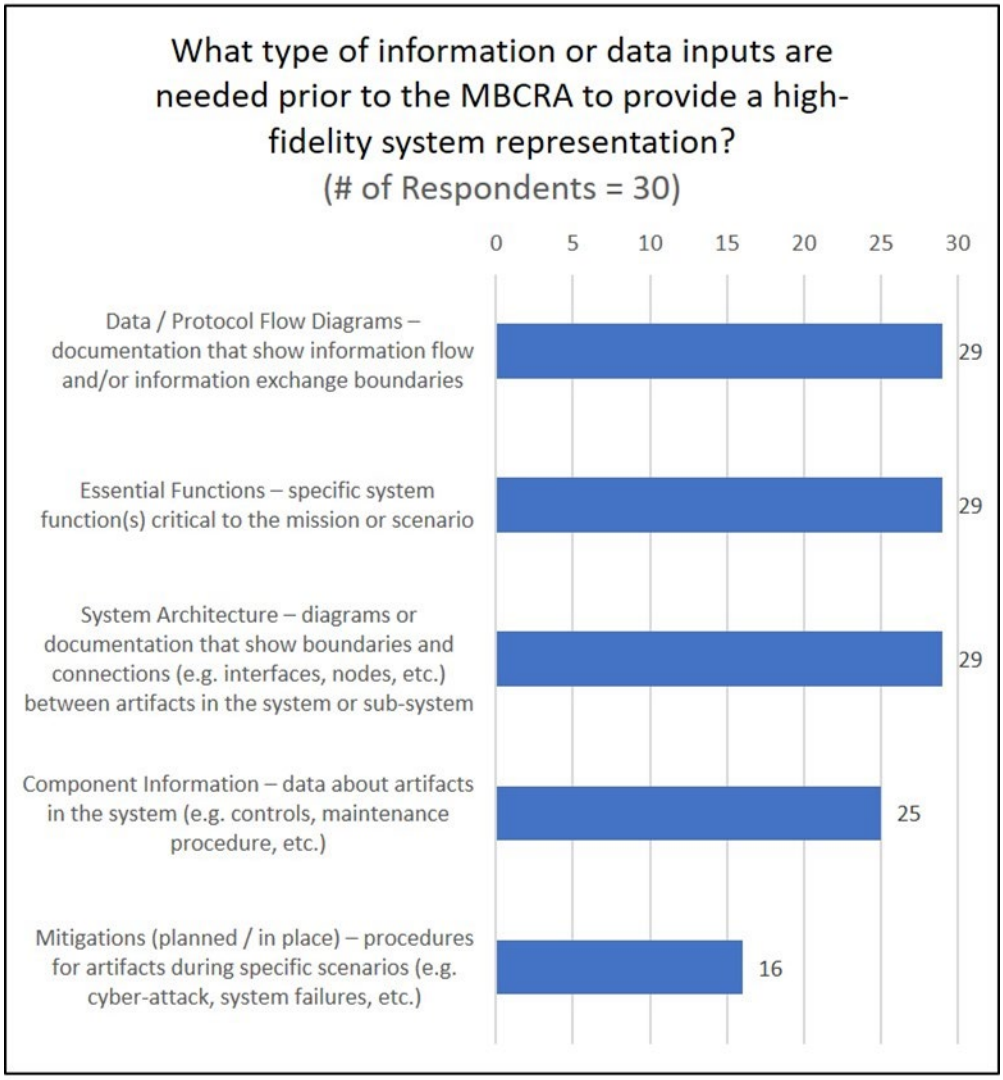


Figure C-10. Survey responses selected for Question 13

Table C-5. Survey responses written for Question 13

Write-in Responses	# of Responses
"Cybersecurity threat information like VOLT".	1
"System Models; DoDAF Views SV-4, SV-5, DIV-2, etc."	1
"User guides for critical systems/components. Hardware and software lists. Ports, Protocols, and Services Management (PPSM) documentation."	1
"Whatever information is available at the time."	1

14. What type of information or data inputs are needed prior to the MBCRA to provide a comprehensive understanding of the threat?

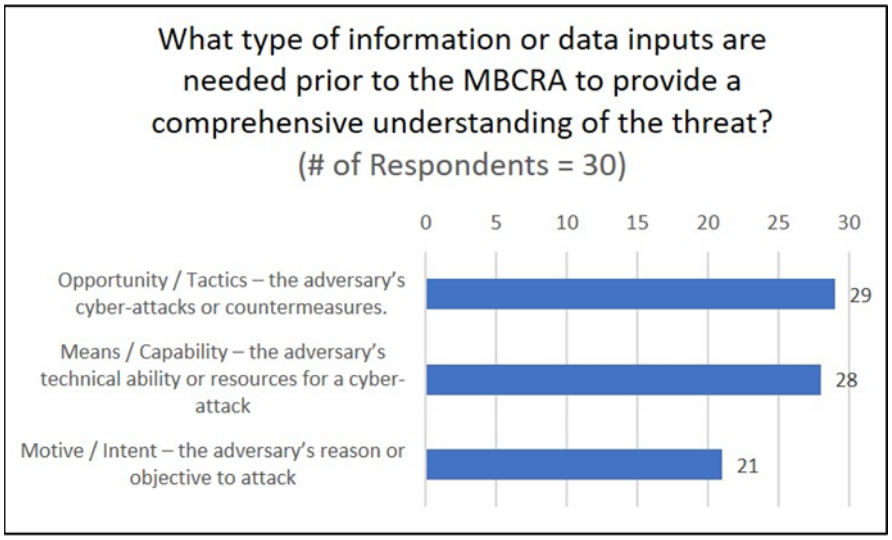


Figure C-11. Survey responses selected for Question 14

Table C-6. Survey responses written for Question 14

Write-in Responses	# of Responses
"All of these items may / may not be needed. Depends on scope of MBCRA."	1
"Assumed access capability."	1
"Suspected or confirmed system information leakage, due to prior successful attacks on the development/sustainment contractor or program office."	1
"Threat models -- CAPEC, ATT&CK, STIX/TAXI."	1

15. Which input data or information is (are) difficult to obtain prior to conducting an MBCRA? (select all that apply)

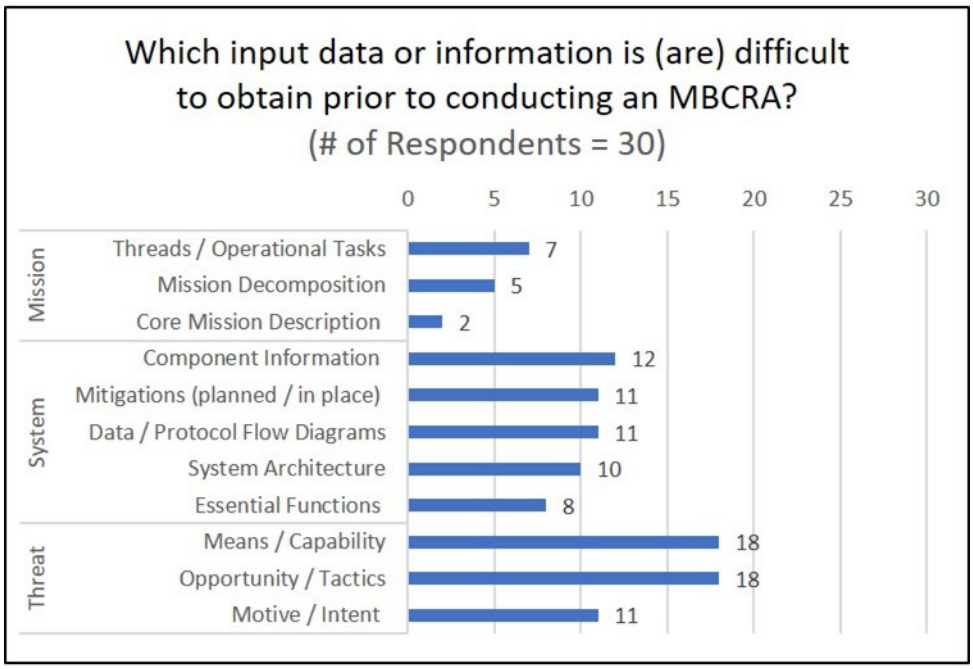


Figure C-12. Survey responses selected for Question 15

Table C-7. Survey responses written for Question 15

Write-in Responses	# of Responses
"Depends on type of system. Scope of MBCRA, prime contract, data rights, Intel availability, and classification."	1
"On-hand cyber support at events."	1
"Past test results for the SUT, as well as interconnected systems."	1

16. Could you explain why the specific MBCRA data input(s) you selected is (are) difficult to obtain? (write-in)

Table C-8. Survey responses written for Question 16

Categorization of Responses	# of Responses
Insufficient level of detail in intelligence data	8
Incomplete documentation, inaccurate or inconsistent data	7
Access to classified information due to personnel's security clearance	5
Identifying personnel who have the required data and knowledge about it	4
Information not defined in early development	4
Access to scope of operational missions	2
Time to receive information	2
Inconsistent configuration management practices by maintainers.	1
System owners have little understanding of how operators use systems	1
Not requesting intelligence information	1
Data rights prohibiting access	1
Personnel/subject matter expert availability	1
Cyber defense (mitigations) involved too late in development	1

* Total respondents = 30.

Questions about MBCRA Results

17. What MBCRA result(s) or output data is(are) valuable? (select all that apply)

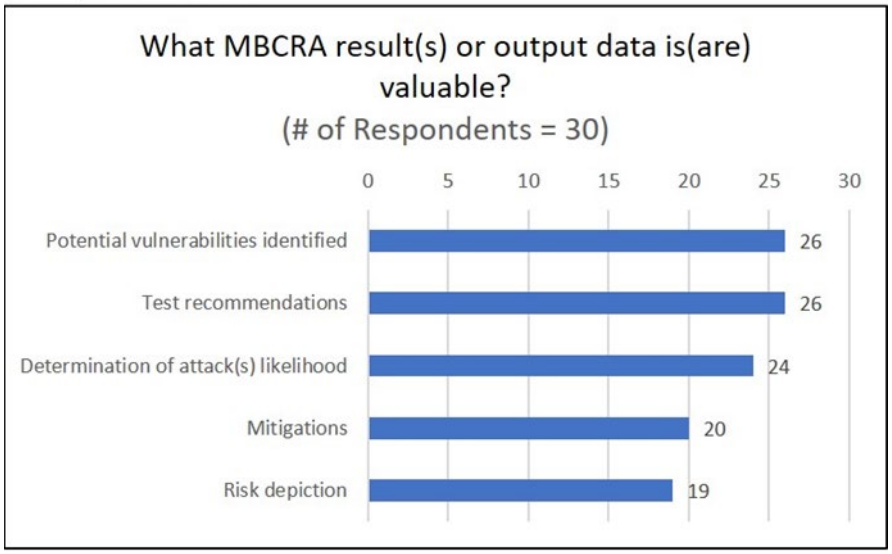


Figure C-13. Survey responses selected for Question 17

Table C-9. Survey responses written for Question 17

Write-in Responses	# of Responses
Attack scenarios/vignettes, mappings of scenarios to cyber requirements (helps programs understand how executing vignettes during cyber test can validate effectiveness of cyber requirements and the need for test support resources)	1
Mission impact	1
The key aspects of the system/network that need to be best protected	1

18. Could you please explain why the specific MBCRA result/data output you selected is(are) valuable?

Table C-10. Survey responses selected for Question 18

Categorization of Responses	# of Responses
Informs test design, strategy	12
Informs how to manage/prioritize cyber risk	9
Informs engineering process, design decisions	7
Provides information to help understand the system in a real-world context	6

* Total respondents = 22.

19. When reporting MBCRA results, which data output format(s) is(are) most useful? (select all that apply)

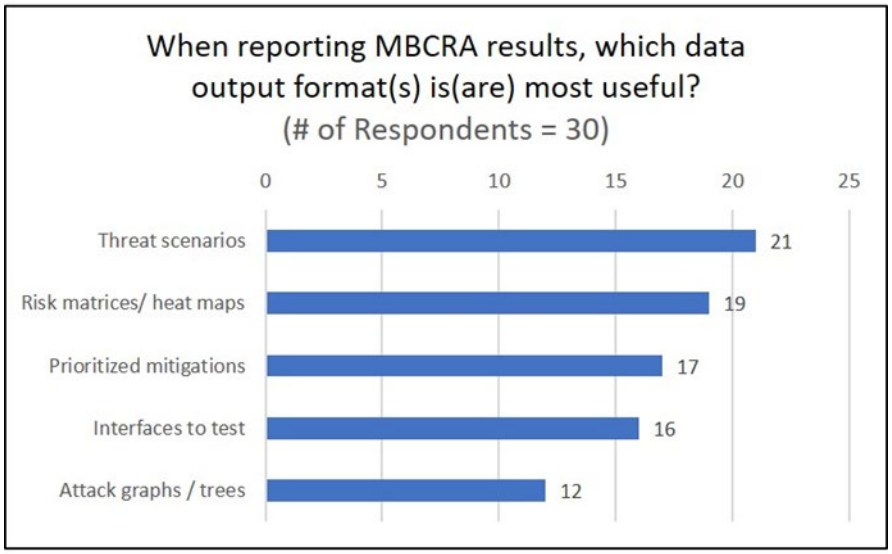


Figure C-14. Survey responses selected for Question 19

Table C-11. Survey responses written for Question 19

Write-in Responses	# of Responses
“Clear written paragraphs - not pictures.”	1
“Cyber Kill Chains.”	1
“Whatever resonates with the customer/audience the most (it's different for everyone).”	1
“Written report with all data presented.”	1

20. Could you explain why the specific data output format is(are) useful?

Table C-12. Survey responses for Question 20

Categorization of Responses	# of Responses
Communication tool to inform stakeholders (e.g., program office, senior leadership)	9
Illustrates results in a focused/easy to understand manner	7
Informs future T&E objectives	6
Communication tool to inform mission planners, operators, system developers	2
Illustrates risk/impact of vulnerabilities in operational context	2
Illustrates risk in standardized format	2
Informs operational testing	2

* Total respondents = 21.

Questions about MBCRA Outcomes

21. In your experience, how frequently have results (when available) from a prior MBCRA been used to inform a later MBCRA? (select one)

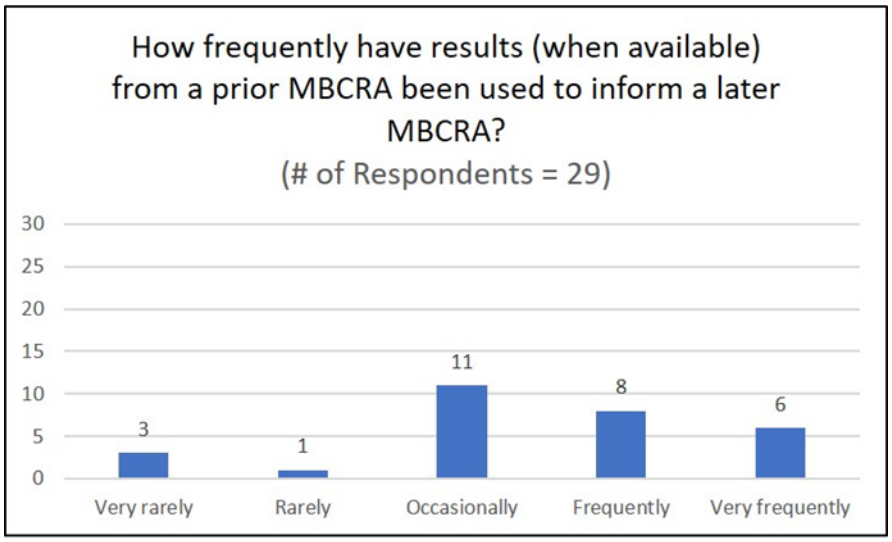


Figure C-15. Survey responses to Question 21

22. The budget for an MBCRA is typically sufficient to conduct an effective assessment. (select one)

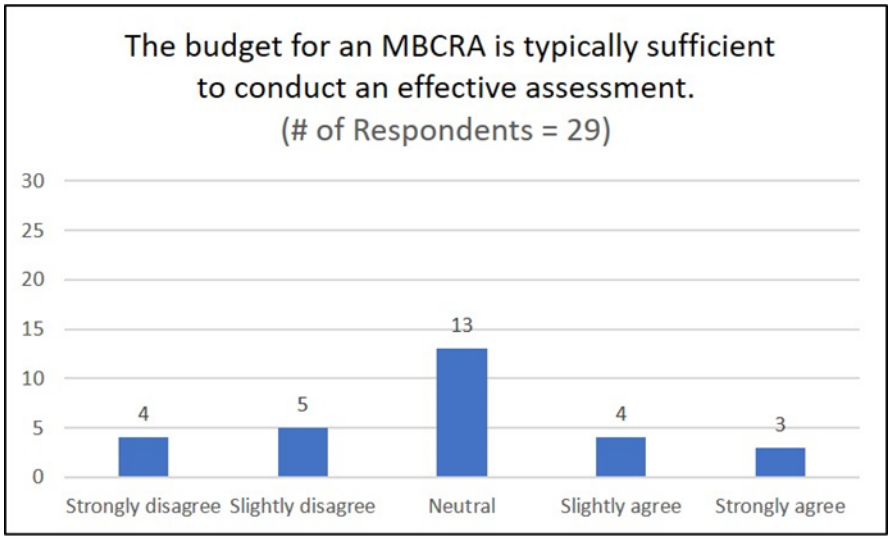


Figure C-16. Survey responses to Question 22

Questions about Respondents' Demographics

23. How would you categorize your employer? (select one)

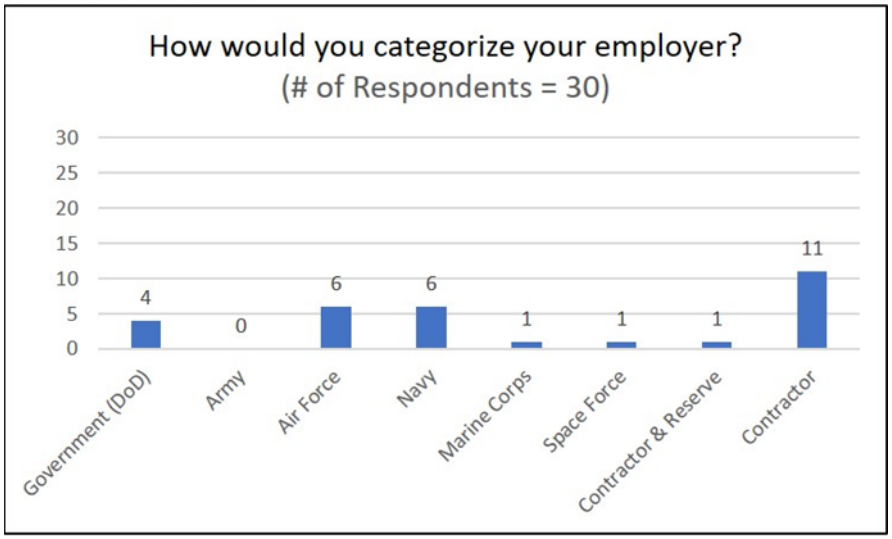


Figure C-17. Survey responses to Question 23

24. What is (are) your current role(s)? (select all that apply)

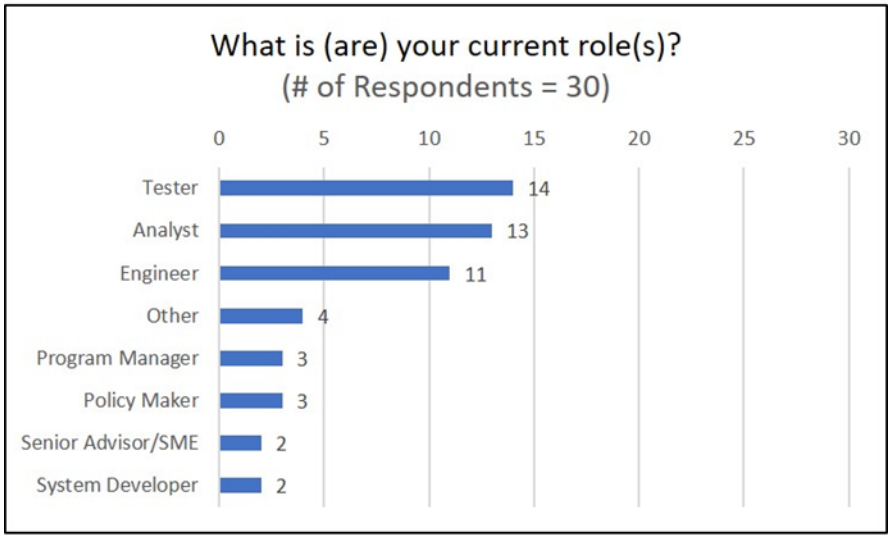


Figure C-18. Survey responses to Question 24

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
06-2022	Paper	START DATE	END DATE

4. TITLE AND SUBTITLE
Analysis of Mission Based Cyber Risk Assessments (MBCRAs) Usage in DoD's Cyber Test & Evaluation

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.; de Naray, Rachel Kuzio.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Institute for Defense Analyses
730 East Glebe Road
Alexandria, Virginia 22305

8. PERFORMING ORGANIZATION REPORT NUMBER
P-33109
H 2022-000221

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER
Ms. Sarah Standard DTE&A		

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A: Cleared for public release by the DoD Office of Prepublication and Security Review, Case 22-S-2752, 1 September 2022

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. This Institute for Defense Analyses (IDA) developed a 30 question survey to better understand the use of and needs from MBCRAs across DoD's cyber test and evaluation community and analyzed the responses. This analysis provides information in an on-going effort to inform DoD's development of evaluation criteria for MBCRA methodologies.

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

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
Rachel Kuzio de Naray	703-933-6556