4900 University Square, Suite 8
Huntsville, Alabama 35816-1829
www.sentar.com
256-430-0860 (V)/256-430-0840 (F)

Information Assurance (IA) Risk Assessment (IARA) Process for Military Systems White Paper

By: Deborah Williams, CISSP, MPA
Larry Johnson, Ph.D.

8/18/2008

This paper is based on work performed for the Missile Defense Agency. Their insight and guidance is acknowledged and greatly appreciated.

TABLE OF CONTENTS

ABSTRACT

Issues concerning Information Assurance (IA) continue to grow in importance and visibility across the Department of Defense (DoD), and the primary considerations revolve around an understanding of IA risk. However, despite the need to understand a true IA risk surrounding an issue or set of issues, methods to assess and communicate that risk are often poorly documented, non-repeatable, and lacking an operational construct. Furthermore, since few decision makers have unlimited resources to apply toward mitigations of IA concerns, making mitigation decisions based on a well grounded understanding of risk is an appropriate way to prioritize limited IA resources and expenditures. While the theory of IA risk assessment is well presented across academic and professional publications, step-by-step processes that allow an analyst to make operationally focused, repeatable, well documented and defendable IA risk assessments are not widely available. The Information Assurance Risk Assessment (IARA) process detailed in this white paper provides a defined methodology to make such risk assessments.

The development of the IARA process stems from the authors' experiences when faced with the need to make determinations on the relationship of IA risks to the operational mission of complex systems-of-systems U.S. military constructs and develop risk-ordered mitigation plans. While IA vulnerability assessment tools often yielded a hard-coded risk score, we found that these ratings were often heavily skewed toward consequence, and lacked the consideration of a meaningful likelihood assessment. Furthermore, we found that the assumptions built into such hard-coded risk ratings were often based on premises and assumptions that may or may not be applicable for the systems that we were trying to assess. We evaluated multiple IA risk assessment models across Government and Academic literature that provided consensus around the common theme of assessing both likelihood and consequence as independent variables in the risk determination process. However, the literature lacked specific guidance on how to make such assessments.

The IARA was developed as a tool to assist IA analysts to make rigorous, operationally focused, defendable and repeatable IA risk assessments. The methodology presented is focused specifically on assessing IA risks for systems that are evaluated against the IA Controls that form the foundation of the Department of Defense's Information Assurance Certification and Accreditation Process (DIACAP). However, the IARA may be used for any IA risk assessment of an individual issue, finding, or concern regardless of its relationship to a defined IA control.

The IARA Process leverages the analysts' understanding of the operational and administrative environment that the system operates within the computing/networked architecture of the system and the relationship of the identified vulnerability/deficiency to the trusted computing path critical to the

system's operational mission. With this knowledge, IARA guides the analyst through a series of determinations that form a two-factored assessment of both the likelihood and consequence of the possible exploit of the identified vulnerability or deficiency. The independently derived likelihood and consequence determinations are then factored together into a risk determination of the deficiency/vulnerability being assessed. The end-result of the IARA process when applied to a set of IA issues within a particular system is a risk-prioritized ranking of the issues that facilities well-grounded decision surrounding mitigation efforts.

While the IARA construct may be used as-is for many systems, it may also be tailored to better fit the specific environment and operational characteristics of the system being assessed. For those wishing to experiment with the IARA, an Excel-based tool that aids in the construction of the individual likelihood and consequence and aggregate risk ratings, it is available free of charge through the Sentar website at http://www.sentar.com.

Information Assurance (IA) Risk Assessment (IARA) Process for Military Systems

1.0 CHALLENGE, PURPOSE AND APPLICABILITY

1.1 Challenge

The emergence and implementation of the Department of Defense's Information Assurance Certification and Accreditation Process (DIACAP) and the associated IA Controls has infused greater rigor and repeatability into the practices of assessing information assurance postures of government systems.[1] By using these controls as the objective benchmarks, a system's security can be measured against consistent and well-defined criteria.

While these controls offer a solid way to measure compliance with applicable standards, they fall short with regard to risk assessments. From a risk perspective, not all controls are created equal. That is, compliance with some controls affords a greater risk reduction than compliance with other controls. Similarly, the costs and time associated with achieving compliance with unique controls vary significantly depending upon conditions inherent in the system and the operational profile of the system. Given these system and environment driven constraints, Information Security analysts need a well-defined, documented repeatable process to assess the risks accruing from non-compliance with the DoD 8500.2 controls.

1.2 Purpose and Applicability

The Information Assurance Risk Assessment (IARA) is intended to provide step-by-step guidance to Information Systems Security professionals across the DoD in their efforts to make meaningful risk assessments based on a documented, defendable and repeatable process. Information Assurance professionals can apply this process to assessments of US military systems. The processes described in this paper facilitate discrete risk assessments for specific IA control non-compliances and IA issues that are found within a system.[2] The objective of IARA is to provide a consistent, methodology that:

- Is appropriate for the multitude of IT systems within military regardless of criticality, scope and mission.
- Is benchmarked against accepted DoD/ Civilian Agency / International / Industry Standards.

[1] Department of Defense Instruction 8500.2, and its companion DoD Information Assurance Certification and Accreditation Process (DIACAP) 8510.01 offer guidance toward assessing the Information Security posture of Military systems and were published in February 2003 and November 2007 respectively

[2] The IARA process described in this white paper does not provide a method to aggregate multiple IA risks into a consolidated IA risk posture for the system at large, or for system-of-systems architectures. These methodologies are available (and have been fielded), but are outside the scope of this paper.

- Facilitates a risk-ordered ranking across multiple non-compliance issues within the same system.
- Supports the development of risk-based Plans of Actions and Milestones (POA&M) development for issue mitigation.
- Supports Certification Determinations.
- Includes system stakeholders as part of the overall process.

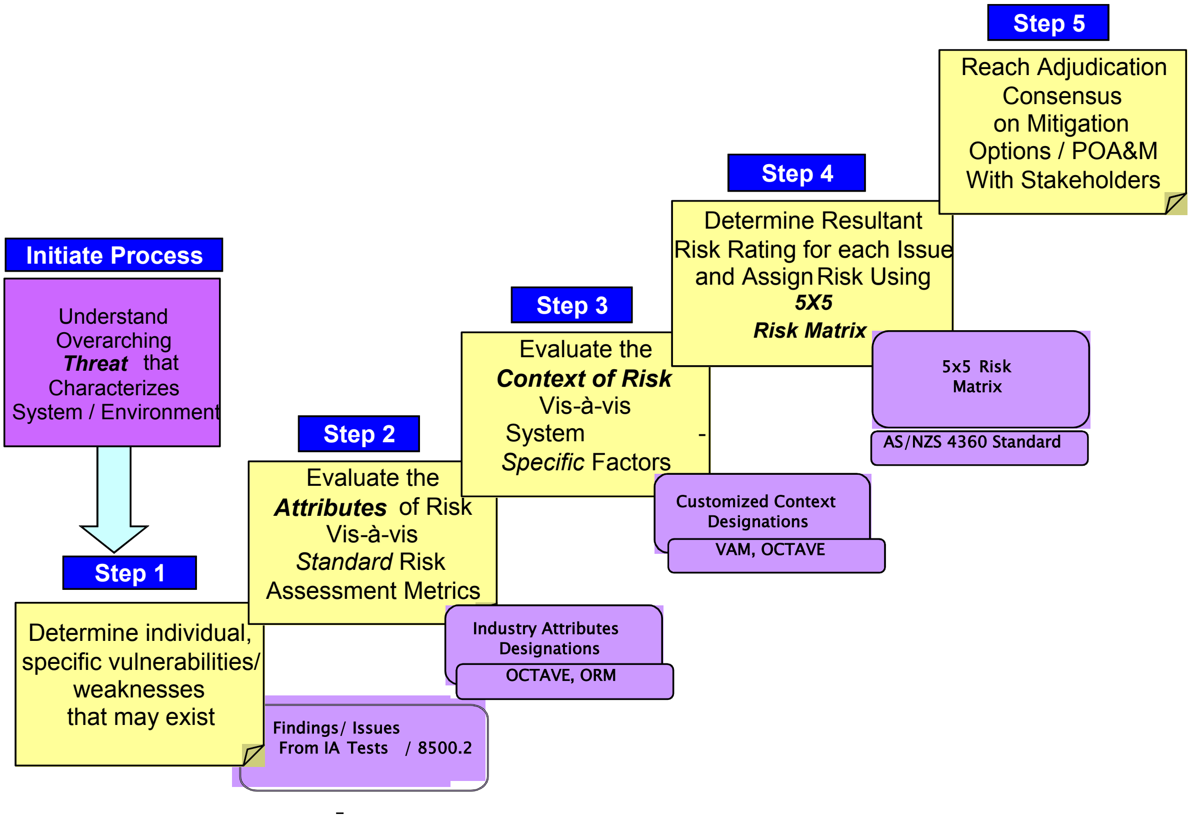
While the IARA is designed to produce well-documented, defendable and repeatable risk assessments, there are some caveats that the user should keep in mind. Solid risk assessments are an outcome of a well-defined process being used by knowledgeable analysts. Best results will come from analysts who have a clear understanding of the following:

- Mission, function and operation of the system being assessed
- Information System Architecture
- Information System's Security Architecture.

A solid grasp of these three critical and inter-related aspects of the system being assessed is critical for a well-founded risk assessment.

2.0 THE IA RISK ASSESSMENT (IARA) PROCESS FLOW

The overall IARA process flow is shown in Figure 2.0.-1 below. It may be used to determine the operational risks associated with IA vulnerabilities identified during Certification and Accreditation testing, and any other risk assessment based upon identified non-compliance with an IA control or other requirement. The IARA process flow begins with an *understanding of the threat* that characterizes the Information System (IS) and its operational environment. This understanding provides the necessary insight into the threat motive, means, and opportunity that is essential for application of the IARA process itself to determine true IA to the operational mission of the system stemming from an identified vulnerability.



Step 5
Reach Adjudication Consensus on Mitigation Options / POA&M With Stakeholders
Step 4
Determine Resultant Risk Rating for each Issue and Assign Risk Using
5X5
Risk Matrix
5x5 Risk Matrix
AS/NZS 4360 Standard
Step 3
Evaluate the ***Context of Risk*** Vis-à-vis System *Specific* Factors
Customized Context Designations
VAM, OCTAVE
Initiate Process
Understand Overarching ***Threat*** that Characterizes System / Environment
Step 2
Evaluate the ***Attributes*** of Risk Vis-à-vis *Standard* Risk Assessment Metrics
Industry Attributes Designations
OCTAVE, ORM
Step 1
Determine individual, specific vulnerabilities/ weaknesses that may exist
Findings/ Issues From IA Tests / 8500.2

Figure 2.0-1: IARA Process Flow

The actual IA risk assessment process flow consists of five sequential steps as indicated in Figure 2.0-2.

Step	Process	Expanded Description of Process
1	Determine the individual, specific IA vulnerabilities that may exist within the system, component or sub-system	An IA analyst, who will document the analysis results as part of the IARA process, makes vulnerability determination. Specific vulnerabilities may stem from C&A testing, other IA Vulnerability testing, or from IAVAs.
2 & 3	Identify the appropriate "Likelihood" and "Consequence" risk factors associated with each vulnerability and failed IA Control, and then determine the resultant overall risk posed by the vulnerability.	Risk determination is made by an IA analyst, who will document the rationale for "Likelihood," "Consequence," and "Risk" determination as part of the IARA process. Section X contains the detailed assessment process for "Likelihood," "Consequence," and "Risk" evaluation.

Step	Process	Expanded Description of Process
4	Assign an Initial Risk Rating [3] and mitigation approach for each failed IA Control or identified vulnerability, based on the results from Steps 2 and Step 3 above, and adjudicate with system stakeholders (developers, system-security engineers, Program Managers and others as appropriate)	The Initial Risk Rating is based on the analyzed risk associated with each failed IA control or other identified IA vulnerability. The analyst assigns an initial risk rating and mitigation approach to each failed control. The risk rating and mitigation approach is finalized when stakeholder adjudication is complete.
5	Develop POA&M, make Certification Determination, and staff with all stakeholders. Results of interactions with stakeholders may introduce new information causing the analyst to adjust the initial risk rating.	Based on the final risk rating reflecting any adjustments reached through adjudication efforts with stakeholders, the IA analyst assigns the final risk rating.

Figure 2.0-2: Detailed Steps in the IARA Process Flow

3.0 SELECTION OF THE APPROPRIATE RISK RATING CRITERIA AND EVALUATION MATRIX

IA vulnerabilities may arise within two considerably different domain contexts. Many IA vulnerabilities stem directly from conditions that are purely in the realm of computer security concerns (e.g., weak patch profiles, incorrect privilege settings, poor passwords, etc.). Alternatively, vulnerabilities may stem from factors that relate to the overall operational environment in which the IS operates, and could affect the overall IA posture but are not directly correlated to computer security vulnerabilities. Vulnerabilities that may not be attributed directly to computer security may include shortcomings in the programmatic (e.g., policies, component documentation, design, etc.), environmental, physical, and/or administrative security posture of an Information System.

This recognition suggests that the analyst must know the proper domain context of each IA Control before conducting a risk assessment of a vulnerability associated with that Control. The analyst must correctly discern between operational risk stemming from vulnerabilities that are sufficient in and of themselves to have a high probability of resulting in a *direct* computer security IA exploit with potential operational consequences, and operational risk stemming from vulnerabilities that create an environment in which an IA weakness could *indirectly* lead to adverse mission consequences.

For the purposes of IARA, the analyst may consider that Computer Security (CS) vulnerabilities are limited to those with a direct IA impact, and the programmatic, environmental, and/or physical/administrative security (PEPA) vulnerabilities may be considered as having an indirect impact. As such, the likelihood and

[3] For DIACAP assessments, this risk rating corresponds to the Severity Code.

consequence determination scales for CS and PEPA based vulnerabilities are different.

Each control as contained within DoDI 8500.2 may be allocated to either the CS or the PEPA grading scale. While the allocation of specific controls may differ for various systems, a general allocation of controls may be based upon the family designator of the controls. Figure 3.0-1 presents a recommended allocation for DoDI 8500.2 controls.

Control Family Heritage	Control Family	Recommended IARA Allocation
DoDI 8500.2	Security Design and Configuration (DC)	PEPA
	Identification and Authentication (IA)	CS
	Enclave and Computing Environment (EC)	CS
	Enclave Boundary Defense EB)	CS
	Physical and Environmental (PE)	PEPA
	Personnel (PR)	PEPA
	Continuity (CO	PEPA
	Vulnerability and Incident Management (VI)	PEPA

Figure 3.0-1: Recommended Allocation of Controls to CS and PEPA Grading Matrices

Separate "Likelihood" and "Consequence" risk assessment criteria and risk evaluation matrices for CS vulnerabilities and PEPA vulnerabilities have been developed for use in the IARA.

4.0 STEP-BY-STEP PROCESS FOR CONDUCTING THE IA RISK ASSESSMENT

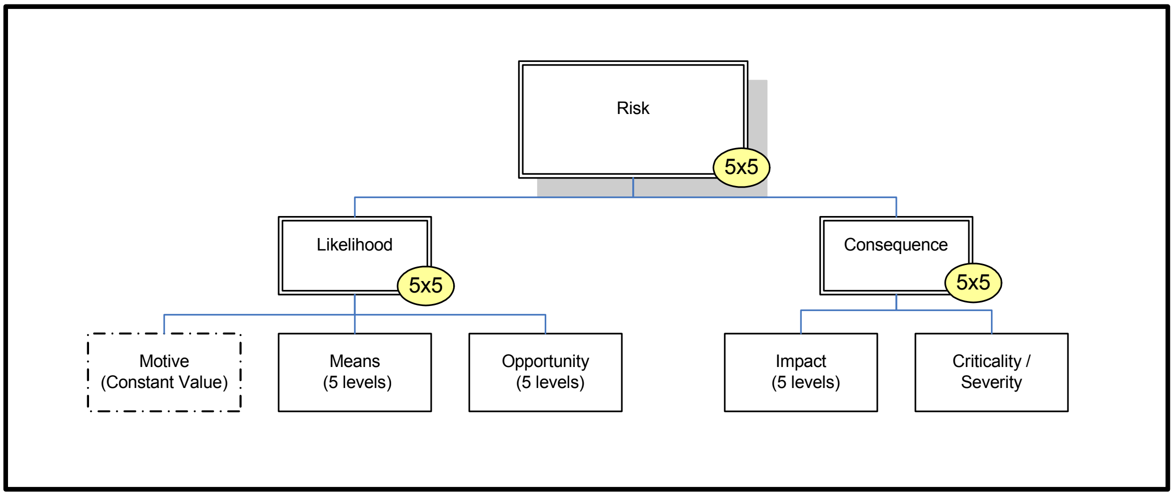


Figure 4.0-1: Likelihood and Consequence Relationships to Risk

The detailed steps required for risk evaluation, and risk assignment are shown in Figure 4.0-1 below.

Step	Action Execution Process	Expanded Description of Process
1	Allocate each failed IA control/IAVA/other identified vulnerability to the correct "Likelihood" and "Consequence" risk rating criteria and evaluation matrix (Computer Security (CS) or Programmatic, Environmental, and/or Physical/Administrative Security (PEPA)).	Using the IA control family allocations guidelines as provided in Figure 5.0-1, the Analyst should evaluate each control within that family to determine its appropriate placement within the CS or PEPA evaluation matrices.
2	For each failed IA control or identified vulnerability, use the appropriate (CS or PEPA) Likelihood rating criteria and evaluation matrix to determine the Likelihood that the failed control/vulnerability can/will be exploited.	Using the appropriate CS or PEPA Likelihood Matrix, the analyst should determine which conditions of means and opportunity best express the likelihood of exploit associated with the control's non-compliance status. Once the Means and Opportunity scores have been established, the resulting likelihood score may be plotted on the Likelihood Evaluation 5X5 matrix.
3	For each failed IA control or identified vulnerability, use the appropriate (CS or PEPA) Consequence rating criteria and evaluation matrix to determine the Consequence to the operational mission of the system(s) should the failed control/vulnerability be exploited.	Using the appropriate CS or PEPA Consequence Matrix, the analyst should determine the Impact and Criticality criteria conditions that best express the consequences of exploit associated with the control's non-compliance status. Once the Impact and Criticality scores has been established, the resulting consequence score may be plotted on the Consequence Evaluation 5X5 matrix.
4	Apply the Likelihood and Consequence assessment results to the Risk evaluation matrix to determine the resultant operational Risk to the system that may stem from each failed IA control.	Using the individually derived likelihood and consequence ratings from Steps 2 and 3, plot these scores on the Risk Assessment Matrix to derive the Risk Rating for the failed control. [4]
6	Based on the risk score, develop POA&M mitigation recommendations of the failed controls and start stakeholder discussions if necessary to derive final risk rating.	Once all failed controls have been assessed, the analyst may use the risk-ordered ratings to prioritize recommended mitigation recommendations.
7	As warranted, make adjustments to the risk ratings based on new information.	As appropriate, engage in further fact-finding with system stakeholders. Where newly provided information warrant a re-consideration, integrate the new information into the assessment, and re-perform the assessment based on the new understandings.
8	Utilize the completed risk assessments for all non-compliant controls to make system mitigation recommendations to the appropriate officials.	Use the prioritized risk ratings to make POA&M recommendations to the appropriate officials.

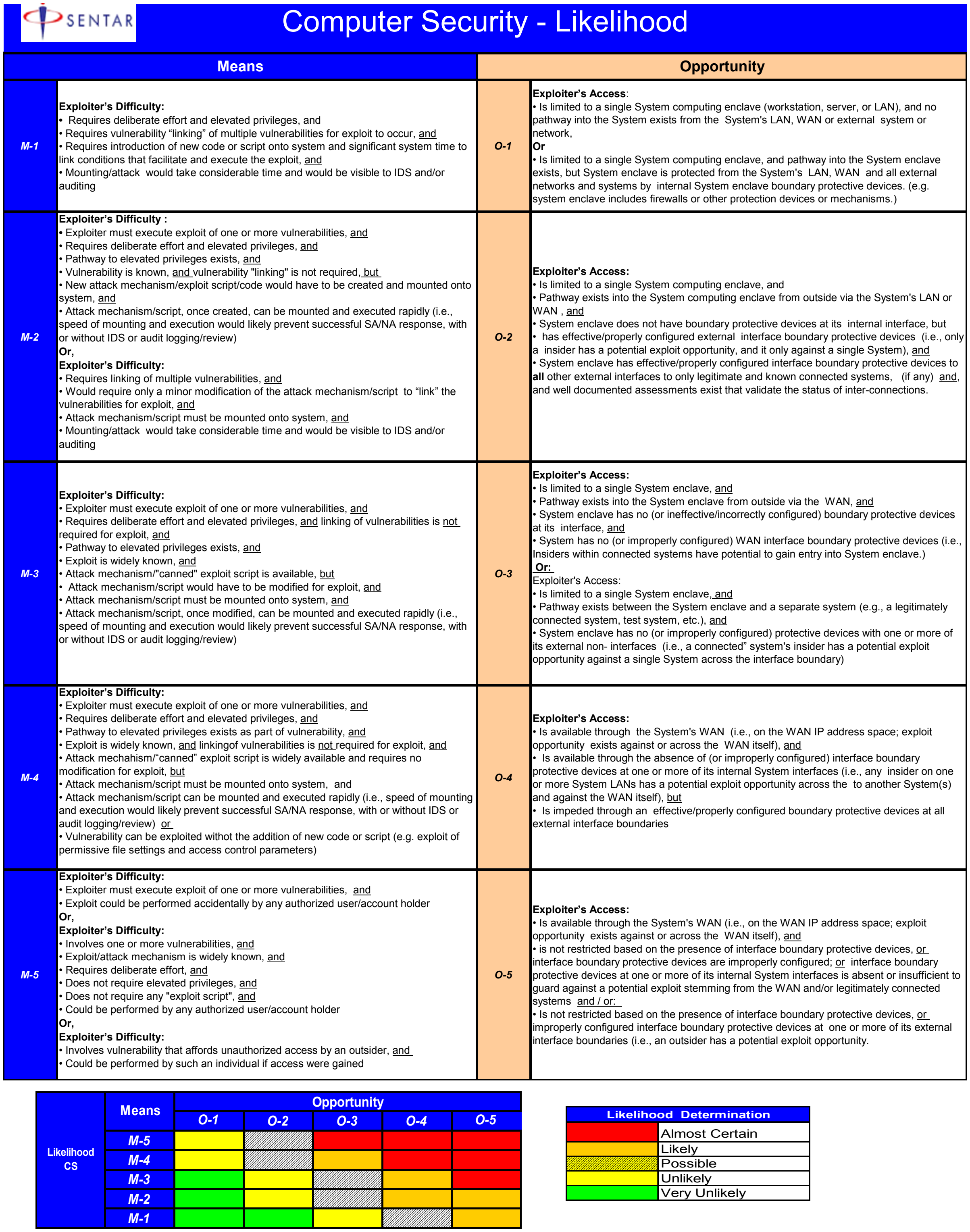
Figure 4.0-2: Detailed Actions for Conducting the IARA

[4] For the DIACAP, the resulting risk color (red, yellow, green) may be used to determine the corresponding severity category of the non-compliance. Red = CAT I, Yellow = CAT II, and Green = CAT III.

5.0 DETAILED DISCUSSION OF IARA "LIKELIHOOD" AND "CONSEQUENCE" ASSESSMENTS FOR AN INDIVIDUAL IA CONTROL NON-COMPLIANCES

Determining the Likelihood Rating of a Failed Control

Once the analyst has determined the appropriate likelihood-rating matrix to use on an identified non-compliance, those conditions on that matrix are assessed to determine the individual Means and Opportunity scores, and the resulting Likelihood Score for the identified non-compliant control. Both the CS and PEPA Likelihood Matrices are presented in Figure 5.0-1.



Computer Security - Likelihood

	Means		Opportunity
M-1	**Exploiter's Difficulty:** • Requires deliberate effort and elevated privileges, and • Requires vulnerability "linking" of multiple vulnerabilities for exploit to occur, and • Requires introduction of new code or script onto system and significant system time to link conditions that facilitate and execute the exploit, and • Mounting/attack would take considerable time and would be visible to IDS and/or auditing	O-1	**Exploiter's Access**: • Is limited to a single System computing enclave (workstation, server, or LAN), and no pathway into the System exists from the System's LAN, WAN or external system or network, **Or** • Is limited to a single System computing enclave, and pathway into the System enclave exists, but System enclave is protected from the System's LAN, WAN and all external networks and systems by internal System enclave boundary protective devices. (e.g. system enclave includes firewalls or other protection devices or mechanisms.)
M-2	**Exploiter's Difficulty :** • Exploiter must execute exploit of one or more vulnerabilities, and • Requires deliberate effort and elevated privileges, and • Pathway to elevated privileges exists, and • Vulnerability is known, and vulnerability "linking" is not required, but • New attack mechanism/exploit script/code would have to be created and mounted onto system, and • Attack mechanism/script, once created, can be mounted and executed rapidly (i.e., speed of mounting and execution would likely prevent successful SA/NA response, with or without IDS or audit logging/review) **Or,** **Exploiter's Difficulty:** • Requires linking of multiple vulnerabilities, and • Would require only a minor modification of the attack mechanism/script to "link" the vulnerabilities for exploit, and • Attack mechanism/script must be mounted onto system, and • Mounting/attack would take considerable time and would be visible to IDS and/or auditing	O-2	**Exploiter's Access:** • Is limited to a single System computing enclave, and • Pathway exists into the System computing enclave from outside via the System's LAN or WAN , and • System enclave does not have boundary protective devices at its internal interface, but • has effective/properly configured external interface boundary protective devices (i.e., only a insider has a potential exploit opportunity, and it only against a single System), and • System enclave has effective/properly configured interface boundary protective devices to **all** other external interfaces to only legitimate and known connected systems, (if any) and, and well documented assessments exist that validate the status of inter-connections.
M-3	**Exploiter's Difficulty:** • Exploiter must execute exploit of one or more vulnerabilities, and • Requires deliberate effort and elevated privileges, and linking of vulnerabilities is not required for exploit, and • Pathway to elevated privileges exists, and • Exploit is widely known, and • Attack mechanism/"canned" exploit script is available, but • Attack mechanism/script would have to be modified for exploit, and • Attack mechanism/script must be mounted onto system, and • Attack mechanism/script, once modified, can be mounted and executed rapidly (i.e., speed of mounting and execution would likely prevent successful SA/NA response, with or without IDS or audit logging/review)	O-3	**Exploiter's Access:** • Is limited to a single System enclave, and • Pathway exists into the System enclave from outside via the WAN, and • System enclave has no (or ineffective/incorrectly configured) boundary protective devices at its interface, and • System has no (or improperly configured) WAN interface boundary protective devices (i.e., Insiders within connected systems have potential to gain entry into System enclave.) **Or:** Exploiter's Access: • Is limited to a single System enclave, and • Pathway exists between the System enclave and a separate system (e.g., a legitimately connected system, test system, etc.), and • System enclave has no (or improperly configured) protective devices with one or more of its external non- interfaces (i.e., a connected" system's insider has a potential exploit opportunity against a single System across the interface boundary)
M-4	**Exploiter's Difficulty:** • Exploiter must execute exploit of one or more vulnerabilities, and • Requires deliberate effort and elevated privileges, and • Pathway to elevated privileges exists as part of vulnerability, and • Exploit is widely known, and linkingof vulnerabilities is not required for exploit, and • Attack mechahism/"canned" exploit script is widely available and requires no modification for exploit, but • Attack mechanism/script must be mounted onto system, and • Attack mechanism/script can be mounted and executed rapidly (i.e., speed of mounting and execution would likely prevent successful SA/NA response, with or without IDS or audit logging/review) or • Vulnerability can be exploited withot the addition of new code or script (e.g. exploit of permissive file settings and access control parameters)	O-4	**Exploiter's Access:** • Is available through the System's WAN (i.e., on the WAN IP address space; exploit opportunity exists against or across the WAN itself), and • Is available through the absence of (or improperly configured) interface boundary protective devices at one or more of its internal System interfaces (i.e., any insider on one or more System LANs has a potential exploit opportunity across the to another System(s) and against the WAN itself), but • Is impeded through an effective/properly configured boundary protective devices at all external interface boundaries
M-5	**Exploiter's Difficulty:** • Exploiter must execute exploit of one or more vulnerabilities, and • Exploit could be performed accidentally by any authorized user/account holder **Or,** **Exploiter's Difficulty:** • Involves one or more vulnerabilities, and • Exploit/attack mechanism is widely known, and • Requires deliberate effort, and • Does not require elevated privileges, and • Does not require any "exploit script", and • Could be performed by any authorized user/account holder **Or,** **Exploiter's Difficulty:** • Involves vulnerability that affords unauthorized access by an outsider, and • Could be performed by such an individual if access were gained	O-5	**Exploiter's Access:** • Is available through the System's WAN (i.e., on the WAN IP address space; exploit opportunity exists against or across the WAN itself), and • is not restricted based on the presence of interface boundary protective devices, or interface boundary protective devices are improperly configured; or interface boundary protective devices at one or more of its internal System interfaces is absent or insufficient to guard against a potential exploit stemming from the WAN and/or legitimately connected systems and / or: • Is not restricted based on the presence of interface boundary protective devices, or improperly configured interface boundary protective devices at one or more of its external interface boundaries (i.e., an outsider has a potential exploit opportunity.

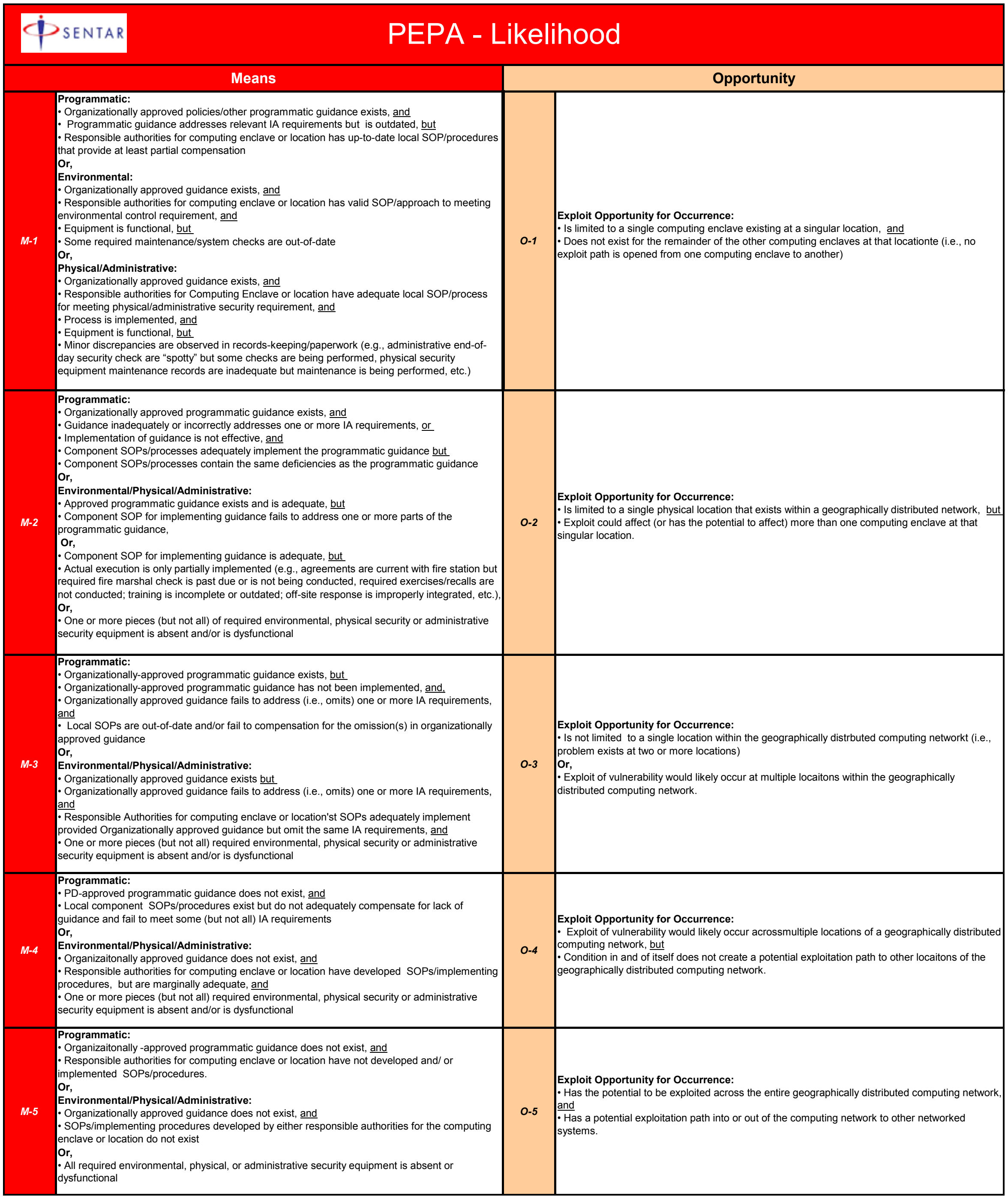
Likelihood CS	Means	Opportunity				
		O-1	O-2	O-3	O-4	O-5
	M-5	🟨	▨	🟥	🟥	🟥
	M-4	🟨	▨	🟧	🟥	🟥
	M-3	🟩	🟨	▨	🟧	🟥
	M-2	🟩	🟨	▨	🟧	🟧
	M-1	🟩	🟩	🟨	▨	🟧

Likelihood Determination	
🟥	Almost Certain
🟧	Likely
▨	Possible
🟨	Unlikely
🟩	Very Unlikely

Figure 5.0-1: Risk Factor Criteria for Computer Security (CS) IA "Likelihood" Assessments

As an example, if we assume that the analyst has determined that the most appropriate Means score is M-2, and the most appropriate Opportunity score is O-5, the resulting likelihood determination will occur at the intersection of M-2 and O-5 That coordinate point is colored orange, and reference to the likelihood determination scale reveals an overall likelihood rating as "likely."

The corresponding matrix for PEPA domain vulnerabilities is shown in Figure 5.0-2.



PEPA - Likelihood

Means		Opportunity	
M-1	**Programmatic:** • Organizationally approved policies/other programmatic guidance exists, and • Programmatic guidance addresses relevant IA requirements but is outdated, but • Responsible authorities for computing enclave or location has up-to-date local SOP/procedures that provide at least partial compensation **Or,** **Environmental:** • Organizationally approved guidance exists, and • Responsible authorities for computing enclave or location has valid SOP/approach to meeting environmental control requirement, and • Equipment is functional, but • Some required maintenance/system checks are out-of-date **Or,** **Physical/Administrative:** • Organizationally approved guidance exists, and • Responsible authorities for Computing Enclave or location have adequate local SOP/process for meeting physical/administrative security requirement, and • Process is implemented, and • Equipment is functional, but • Minor discrepancies are observed in records-keeping/paperwork (e.g., administrative end-of-day security check are "spotty" but some checks are being performed, physical security equipment maintenance records are inadequate but maintenance is being performed, etc.)	O-1	**Exploit Opportunity for Occurrence:** • Is limited to a single computing enclave existing at a singular location, and • Does not exist for the remainder of the other computing enclaves at that locationte (i.e., no exploit path is opened from one computing enclave to another)
M-2	**Programmatic:** • Organizationally approved programmatic guidance exists, and • Guidance inadequately or incorrectly addresses one or more IA requirements, or • Implementation of guidance is not effective, and • Component SOPs/processes adequately implement the programmatic guidance but • Component SOPs/processes contain the same deficiencies as the programmatic guidance **Or,** **Environmental/Physical/Administrative:** • Approved programmatic guidance exists and is adequate, but • Component SOP for implementing guidance fails to address one or more parts of the programmatic guidance, **Or,** • Component SOP for implementing guidance is adequate, but • Actual execution is only partially implemented (e.g., agreements are current with fire station but required fire marshal check is past due or is not being conducted, required exercises/recalls are not conducted; training is incomplete or outdated; off-site response is improperly integrated, etc.), **Or,** • One or more pieces (but not all) of required environmental, physical security or administrative security equipment is absent and/or is dysfunctional	O-2	**Exploit Opportunity for Occurrence:** • Is limited to a single physical location that exists within a geographically distributed network, but • Exploit could affect (or has the potential to affect) more than one computing enclave at that singular location.
M-3	**Programmatic:** • Organizationally-approved programmatic guidance exists, but • Organizationally-approved programmatic guidance has not been implemented, and, • Organizationally approved guidance fails to address (i.e., omits) one or more IA requirements, and • Local SOPs are out-of-date and/or fail to compensation for the omission(s) in organizationally approved guidance **Or,** **Environmental/Physical/Administrative:** • Organizationally approved guidance exists but • Organizationally approved guidance fails to address (i.e., omits) one or more IA requirements, and • Responsible Authorities for computing enclave or location'st SOPs adequately implement provided Organizationally approved guidance but omit the same IA requirements, and • One or more pieces (but not all) required environmental, physical security or administrative security equipment is absent and/or is dysfunctional	O-3	**Exploit Opportunity for Occurrence:** • Is not limited to a single location within the geographically distrbuted computing networkt (i.e., problem exists at two or more locations) **Or,** • Exploit of vulnerability would likely occur at multiple locaitons within the geographically distributed computing network.
M-4	**Programmatic:** • PD-approved programmatic guidance does not exist, and • Local component SOPs/procedures exist but do not adequately compensate for lack of guidance and fail to meet some (but not all) IA requirements **Or,** **Environmental/Physical/Administrative:** • Organizaitonally approved guidance does not exist, and • Responsible authorities for computing enclave or location have developed SOPs/implementing procedures, but are marginally adequate, and • One or more pieces (but not all) required environmental, physical security or administrative security equipment is absent and/or is dysfunctional	O-4	**Exploit Opportunity for Occurrence:** • Exploit of vulnerability would likely occur acrossmultiple locations of a geographically distributed computing network, but • Condition in and of itself does not create a potential exploitation path to other locaitons of the geographically distributed computing network.
M-5	**Programmatic:** • Organizaitonally -approved programmatic guidance does not exist, and • Responsible authorities for computing enclave or location have not developed and/ or implemented SOPs/procedures. **Or,** **Environmental/Physical/Administrative:** • Organizationally approved guidance does not exist, and • SOPs/implementing procedures developed by either responsible authorities for the computing enclave or location do not exist **Or,** • All required environmental, physical, or administrative security equipment is absent or dysfunctional	O-5	**Exploit Opportunity for Occurrence:** • Has the potential to be exploited across the entire geographically distributed computing network, and • Has a potential exploitation path into or out of the computing network to other networked systems.

	Means	Opportunity				
		O-1	*O-2*	*O-3*	*O-4*	*O-5*
Likelihood PEPA	*M-5*	🟨	▨	🟧	🟥	🟥
	M-4	🟨	▨	🟧	🟧	🟥
	M-3	🟩	🟨	▨	🟧	🟥
	M-2	🟩	🟩	🟨	▨	🟧
	M-1	🟩	🟩	🟩	🟨	▨

Likelihood Determination	
🟥	Almost Certain
🟧	Likely
▨	Possible
🟨	Unlikely
🟩	Very Unlikely

Figure 5.0-2: Risk Factor Criteria for Programmatic, Environmental, and/or Physical/Administrative Security (PEPA) IA "Likelihood" Assessments

The usage of the PEPA likelihood table follows the same process described above, and facilitates the analysts' individual ratings of Means and Opportunity to combine into an overall likelihood score.

Determining the Consequence Rating of a Failed Control

After completing the Likelihood portion of the risk assessment with the appropriate CS or PEPA Matrix, the analyst then turns attention to the consequence side of the equation, Figure 5.0-3. After determining the appropriate consequence matrix to use on an identified non-compliance, the analyst assesses those conditions on that matrix to determine the individual Impact and Criticality scores, and the resulting Consequence Score for the identified non-compliant control. Note that the Impact portion of the consequence assessment incorporates the DIACAP defined impacts as associated to the controls.

Computer Security - Consequence

Impact Code		Criticality	
I-1	Non Compliant Control Rating: • Tool Rating: Low (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Low.	*C-1*	**Exploit consequences:** • Are limited to a single system within a defined computing enclave, and exploit could impair that system's ability to provide required measures of availability, confidentiality or integrity for a short time; but the short term loss of availability, confidentiality or integrity **could not** impede the required attributes of availability, confidentiality or integrity across the system or network as a whole. **Or,** **Exploit consequences:** • Could impede the required attributes of availability, confidentiality or integrity across the system or network as a whole, but • Complimentary and effective safegards are in place to prevent/mitigate exploit
I-2	**Non Compliant Control Rating:** • Tool Rating: Medium/High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Low or • Tool Rating: Medium/High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Medium, but complementary protective measures exist that mitigate impact of exploit.	*C-2*	**Exploit consequences:** • Are limited to a single system within a defined computing enclave, and exploit could impair that system's ability to provide required measures of availability, confidentiality or integrity for a short time; but the short term loss of availability, confidentiality or integrity **is unlikely to** impede the required attributes of availability, confidentiality or integrity across the system or network as a whole.
I-3	**Non Compliant Control Rating:** • Tool Rating: Low/Medium (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Medium.	*C-3*	**Exploit consequences:** • Are limited to a single system or multiple systems within a defined computing enclave, and exploit could impair those system's ability to provide required measures of availability, confidentiality or integrity for a short time; and the short term loss of availability, confidentiality or integrity may possibly impede the required attributes of availability, confidentiality or integrity across the system or network as a whole; but such an impedement is unlikely to result in operational impacts to the system(s) or network as a whole. **Or,** • Could impact the entire network or system's ability to provide required measures of availability, confidentiality or integrity for a short time, **but** • the overall operational mission of the system is unlikely to be impeded, **and** alternative measures are in place that provide for a work-around should the system be unavailable for a short time.
I-4	**Non Compliant Control Rating::** • Tool Rating: High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: Medium or • Tool Rating: High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: High, but complementary protective measures exist that mitigate impact of exploit or NIST defined medium baseline control measures are applicable, but protective measures exist that mitigate impact of exploit.	*C-4*	**Exploit consequences:** • May be limited to a single system or computing enclave, but that single system / computing enclave is critical to the operational mission of the system(s) / network. and impeded capabilities to provide required measures of availability, confidentiality or integrity could extent beyond a short time, or impeded measures of availability, confidentialty or integrity for even a short time are likely to adversly impact the overall operational mission of the system(s)/ network. **Or,** • Could impact the entire network or system's ability to provide required measures of availability, confidentiality or integrity for a short time, and • It is possible that the impedement of required levels of availability, confidentiality or integrity will impede the overall operational mission of the system(s) / network. **and** altenative measures could be developed that would provide for a work-around should the system be unavailable for a short time.
I-5	**Non Compliant Control Rating:** • Tool Rating: Low/Medium/High (or equivalent) (if applicable), and • DIACAP Knowledge Base Impact Code: High.	*C-5*	**Exploit consequences:** • Will impact multiple systems / computing enclaves / networks that are critical to the operational mission of the system(s) / network. and impeded capabilities to provide required measures of availability, confidentiality or integrity for even a short time are very likely to adversly impact the overall operational mission of the system(s) / network.

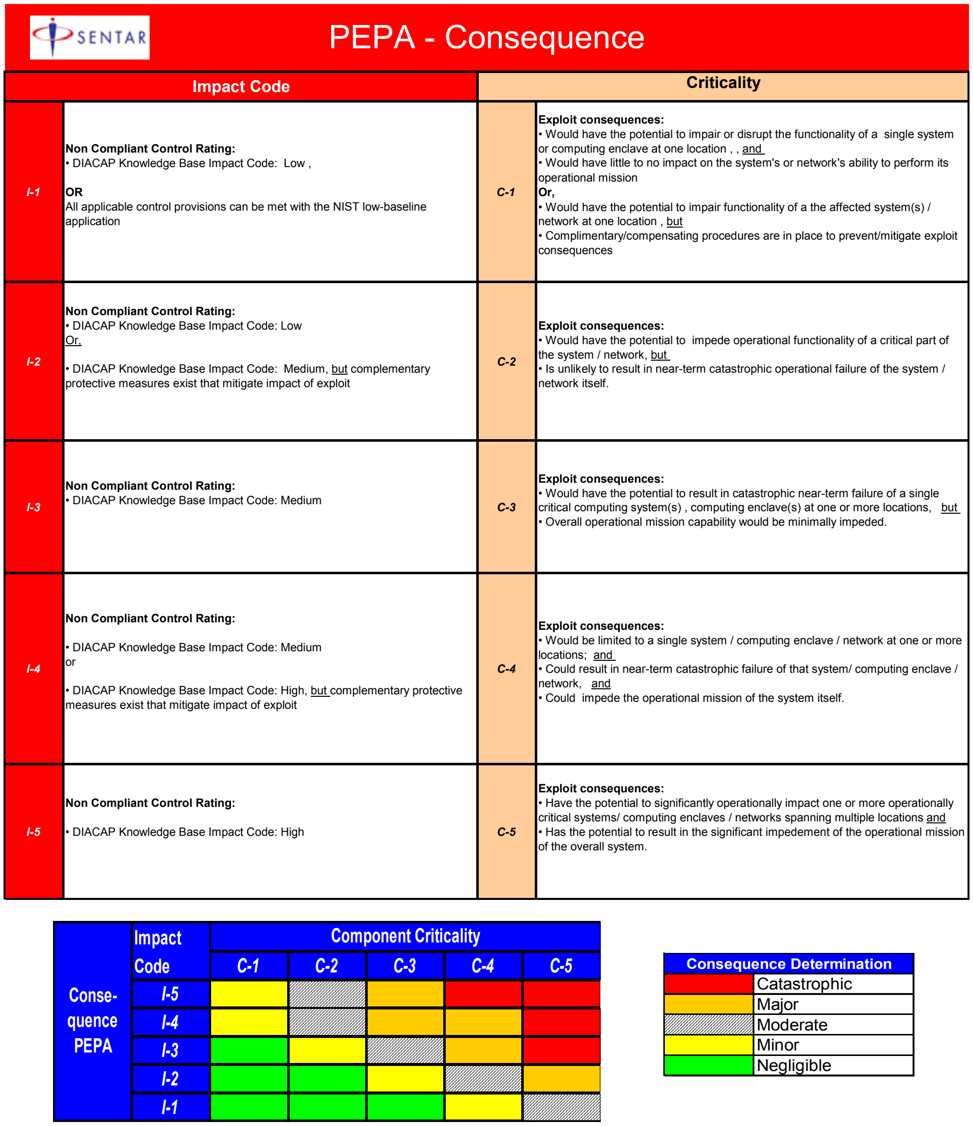
	Tool/Impact	Component Criticality				
	Code	*C-1*	*C-2*	*C-3*	*C-4*	*C-5*
Conse-quence CS	*I-5*	🟨	▨	🟥	🟥	🟥
	I-4	🟨	▨	🟧	🟥	🟥
	I-3	🟩	🟨	▨	🟧	🟥
	I-2	🟩	🟨	▨	🟧	🟧
	I-1	🟩	🟩	🟨	▨	🟧

Consequence Determination	
🟥	Catastrophic
🟧	Major
▨	Moderate
🟨	Minor
🟩	Negligible

Figure 5.0-3: Risk Factor Criteria for Computer Security IA "Consequence" Assessments

The Consequence criteria tables are used in the same manner as the Likelihood criteria tables previously discussed. After determining the best fit for individual Impact and Criticality criteria, these points are then plotted on the Consequence 5X5 Matrix. Using the matrix in 5.0-3 as an example, we shall assume that the analyst grades the Impact as "I-3" and the Criticality as "C-2." Plotting those two coordinates on the Consequence 5X5 matrix reveals a code of "yellow." Reference to the Consequence Determination legend attributes a "yellow" to a Consequence determination of "Minor."

Figure 5.0-4 should be used to determine the applicable impact and criticality factors for each PEPA-related failed IA control. The use of the PEPA Consequence matrix is the same as that detailed in the previous discussion on the CS Consequence matrix.



SENTAR

PEPA - Consequence

Impact Code		Criticality	
I-1	**Non Compliant Control Rating:** • DIACAP Knowledge Base Impact Code: Low , **OR** All applicable control provisions can be met with the NIST low-baseline application	C-1	**Exploit consequences:** • Would have the potential to impair or disrupt the functionality of a single system or computing enclave at one location , , and • Would have little to no impact on the system's or network's ability to perform its operational mission **Or,** • Would have the potential to impair functionality of a the affected system(s) / network at one location , but • Complimentary/compensating procedures are in place to prevent/mitigate exploit consequences
I-2	**Non Compliant Control Rating:** • DIACAP Knowledge Base Impact Code: Low Or, • DIACAP Knowledge Base Impact Code: Medium, but complementary protective measures exist that mitigate impact of exploit	C-2	**Exploit consequences:** • Would have the potential to impede operational functionality of a critical part of the system / network, but • Is unlikely to result in near-term catastrophic operational failure of the system / network itself.
I-3	**Non Compliant Control Rating:** • DIACAP Knowledge Base Impact Code: Medium	C-3	**Exploit consequences:** • Would have the potential to result in catastrophic near-term failure of a single critical computing system(s) , computing enclave(s) at one or more locations, but • Overall operational mission capability would be minimally impeded.
I-4	**Non Compliant Control Rating:** • DIACAP Knowledge Base Impact Code: Medium or • DIACAP Knowledge Base Impact Code: High, but complementary protective measures exist that mitigate impact of exploit	C-4	**Exploit consequences:** • Would be limited to a single system / computing enclave / network at one or more locations; and • Could result in near-term catastrophic failure of that system/ computing enclave / network, and • Could impede the operational mission of the system itself.
I-5	**Non Compliant Control Rating:** • DIACAP Knowledge Base Impact Code: High	C-5	**Exploit consequences:** • Have the potential to significantly operationally impact one or more operationally critical systems/ computing enclaves / networks spanning multiple locations and • Has the potential to result in the significant impedement of the operational mission of the overall system.

Conse-quence PEPA	Impact Code	Component Criticality				
		C-1	C-2	C-3	C-4	C-5
	I-5	🟨	▨	🟧	🟥	🟥
	I-4	🟨	▨	🟧	🟧	🟥
	I-3	🟩	🟨	▨	🟧	🟥
	I-2	🟩	🟩	🟨	▨	🟧
	I-1	🟩	🟩	🟩	🟨	▨

Consequence Determination	
🟥	Catastrophic
🟧	Major
▨	Moderate
🟨	Minor
🟩	Negligible

Figure 5.0-4: Risk Factor Criteria for Programmatic, Environmental, and/or Physical/Administrative Security (PEPA) IA "Consequence" Assessments

Compiling the IA Risk Rating for the Failed Control

Once the analyst has completed the individual ratings for both likelihood and consequence for the non-compliant control, the next step is pulling together these two independent ratings for an overall risk-rating for the failed control. Using the example ratings for a failed Computer Security (CS) control, as illustrated in Figures 5.0-1 and 5.0-3, we have the input necessary to make the initial risk assessment. As illustrated in Figure 5.0-5, the analyst has determined the Likelihood rating be "Likely" and the Consequence rating to be "Minor." These two coordinates are then carried into the Likelihood and Consequence 5X5 matrix and plotted. The resulting risk rating falls into the yellow category, suggesting a CAT-II risk within the context of a DIACAP assessment.

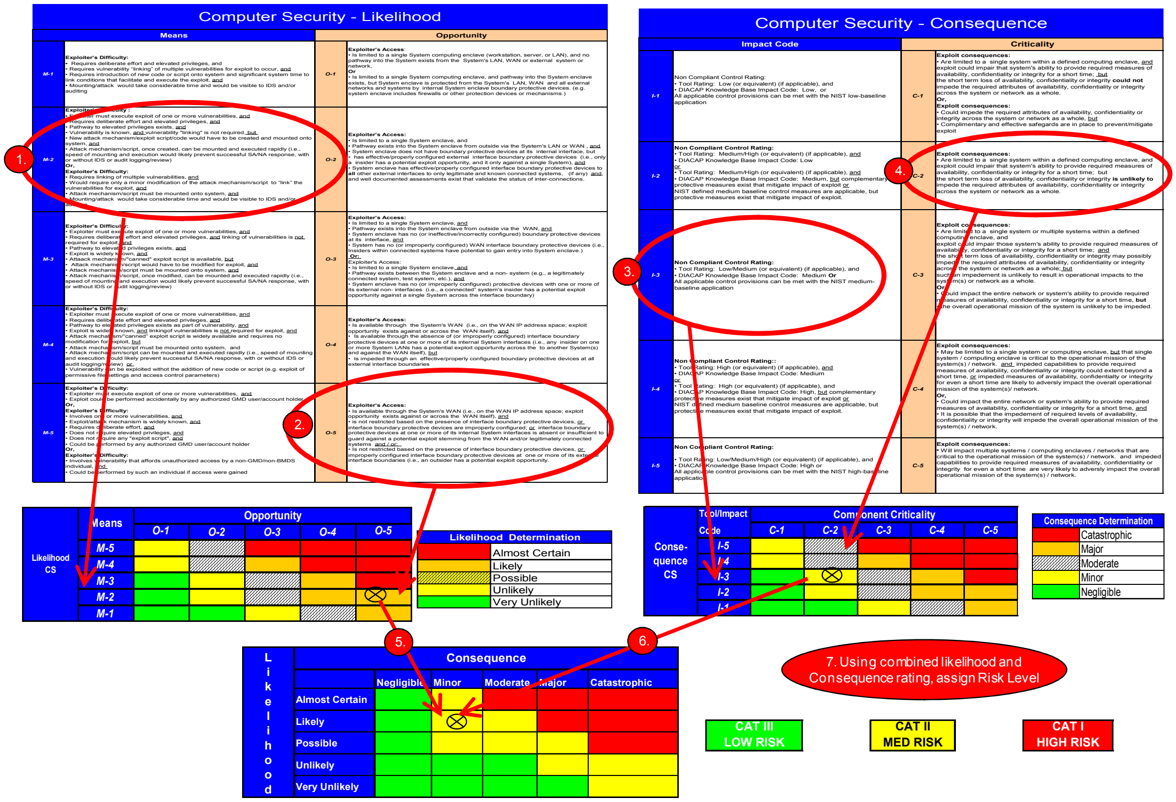


Figure 5.0-5: Pulling Together Likelihood and Consequence to Assess Risk on a Failed Control

6.0 CONCLUSIONS

While the IARA process may be extended to IA risks within systems existing within other public and private sector concerns, the construction of the matrix tables and associated weightings have been developed with a particular focus to IA risk assessments for U.S. military arenas. Similarly, the IARA process as described here-in has been limited to the discussion of determining risks stemming from individual instances of IA control non-compliance and IA issues. Complementary processes are available that facilitate the aggregation of risks to larger systems, and systems-of-system architectures. It is the author's intent that this IARA process might be used as presented, or tailored to better fit the specific needs of the organization that chooses to apply it to their Information Assurance Risk Processes.

7.0 REFERENCES

1. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

2. DoDI 8510.01 " DoD Information Assurance Certification and Accreditation Process (DIACAP); November 28, 2007.

3. "DIACAP IA Compliance Assessment Tool (IA CAT)," The Mitre Corporation, October 2006

4. The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE); by the Carnegie Mellon Computer Emergency Response Team (CERT): As expressed by "Managing Information Security Risks: The OCTAVE Approach", Christopher Alberts and Audrey Dorofee; 2003.

5. The Vulnerability Assessment & Mitigation Methodology: Prepared for the Defense Advanced Research Projects Agency (DARPA) by the RAND National Defense Research Institute: Philip S. Anton, Robert H. Anderson, Richard Mesie, Michael Scheieim: 2003

6. The Australian / New Zealand Standard for Risk Management (AS/NZS 4360:2004)