Command Cyber Readiness Inspection

Risk Indicator Guide

Version 1, Revision 5
Current as of 13 August 2018

Department of Defense Information Networks
Readiness and Security Inspections (DRSI)
Chambersburg, Pennsylvania

Document ID	SOP Ownership	Effective Date	Next Review Date
DoDIN-RSI-CCRI-RISKIND	DoDIN Readiness and Security Inspections	1 October 2014	30 September 2018
	Authors	Revision Date	
	DRSI R & SI RS3	09 February 2018	

REVISION RECORD			
Version	**Primary Author**	**Description of Version**	**Date Completed**
V1R1	D. Wellman	Added new Background; discussion for each Risk Item; and new Appendix A, Risk Assessment	07/21/2014
V1R1	FS21 staffing	All Paragraphs impacted.	07/28/2014
V1R1	D. Wellman	Header, PM Risk Item and Appendix A	08/15/2014
V1R1	FS21 staffing	All Paragraphs impacted	09/19/2014
V1R2	P. Fedorczyk	Risk Assessment	10/17/2014
V1R2	D. Wellman	Risk Assessment	10/24/2014
V1R3	RS5 and USCC Meeting	Wording changes	11/19/2014
V1R3	A. Enfusse	Phase IV Updates	12/12/2014
V1R4	D. Wellman	Added Risk Indicator Items 3.2.15 and 3.2.16	10/21/2015
V1R4	D. Wellman	Changed Risk Indicator Item 3.2.16	12/4/2015
V1R5	M. Bobbs	Updated to reflect organizational change from DISA to JFHQ-DODIN	02/09/2018
	D. Ceithamer	Updated 3.2 CMRS and Risk Report date from 11.5 business days to 45 calendar days	08/13/18

Table of Contents

1. PURPOSE

To provide guidance for completing the Risk Indicator during a Command Cyber Readiness Inspection (CCRI).

2. BACKGROUND

Within the Department of Defense, cyber security risk means vulnerability to network intrusions that will result in data loss or system failures leading to interruption in operations, compliance violations, or the loss of network services.

A risk consists of a vulnerability that can be exploited by a realistic threat to adversely affect a system (asset, host or network). Thus, vulnerabilities must be paired with a likelihood that the vulnerability can be exploited resulting in an adverse impact on the system or network. In each such pairing, the relationship can be deemed high, medium or low. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 rev 1, **Guide for Conducting Risk Assessments,** details the risk assessment process and that approach is recommended.

The Risk Indicator, first introduced in Phase III of the CCRI, is a tool used to assist the site in the process of identifying risks, assessing the impact of these risks, and developing a plan to manage and mitigate these risks. The Risk Indicator is made up of Risk Items. This document explains the rationale behind each Risk Item identified and how it is scored and briefed during a CCRI.

Translating the result of any self-assessment or inspection which focuses on cyber security into operational impact and operational risks has always been a challenge. While compliance with systems configurations requirements, patching discipline and best practices designed to mitigate known vulnerabilities provide a start for identifying and reducing risks, compliance is not the only answer to the challenges associated with risk identification and risk management.

Armed with this information, the next step is to assess the threat. Many types of threat sources can be considered. For example, a single, broad-threat source such as phishing and distributed denial of service attacks based upon known adversarial tactics and techniques or a single threat source such as a trusted insider divulging specific information on the technology, location and status of key systems. Judgments of threat sources and their impact may vary from worst case scenarios to best-case projections.

How to identify, quantify, and mitigate cyber security risks are questions often left to the technical experts in an organization; however, for DoD organizations, input from leaders responsible for mission accomplishment must be brought to bear. The judgments as to low, medium, or high regarding likelihood of exploitation and impact are admittedly subjective judgments. Thus, judgments as to the exploitation of cyber security vulnerabilities are best arrived at by informed technical and leadership personnel working in a collaborative manner.

Cyber Security Risk Management (CSRM) is concerned with the process of managing (reducing) potentially harmful uncertain events due to the lack of cyber security. Key methods for managing cyber security risks include: (1) the efficient use of resources, (2) internal controls, (3) information sharing, (4) technical improvements, and (5) behavioral/ organizational improvements.

The Risk Indicator is part of the final CCRI Compliance Report; however, it is not a factor in determining the final CCRI grade or score. Based upon results from Technology reviews, CND Directives compliance, Contributing Factors evaluation and personal observations, CCRI Team Leads (TL) will provide a Risk Indicator score as part of a CCRI compliance report. As such, this document is a guide to properly complete the Risk Indicator worksheet in the nSpect tool.

3. PROCEDURES

3.1 General

The Risk Indicator is a tool to provide an initial indicator of areas of risk based on information gathered during a CCRI. This information is then analyzed by the Site/Service/Agency being inspected and by their Cyber component to develop an overall Risk Assessment showing the site's risk to the DoDIN as expressed with a numerical score and a rating of High, Medium or Low.

The Risk Indicator matrix portion of the nSpect tool is, at times, redundant to CCRI findings itemized in the Risk Indicator. This is intentional. The Risk Indicator can never be Zero and this too is intentional. The overall goal is to initiate a greater awareness that given today's technology, what is done on DoD networks is inherently risky. At this time, this state of affairs requires leaders and technologists to continuously monitor the posture of their networks and seek the tactics, techniques, and procedures to enhance its ability to repel adversaries and provide for secure mission accomplishment.

The Risk Indicator items scored during a CCRI consists of:

1. Number of findings from all severity categories reported for each network during the CCRI.
2. Traditional/Network Security
3. Antivirus Definition Signature File age
4. Host Based Security System (HBSS) Compliance with required ePolicy Orchestrator (ePO) Server version
5. HBSS with required Point Products and version
6. Continuity of Operations Plan (COOP) Requirements
7. Computer Network Defense Service Provider (CNDSP) Alignment and Relationship
8. Cyber Security Awareness

9. Dated Category I Vulnerabilities
10. Cross Domain Solution Security Posture
11. Operational Readiness Inspections (ORI) and Exercise
12. Target Value for Threat Vectors – Applies to Site and Mission
13. Presence of vulnerable Program Managed Systems on Network
14. Presence of End of Life Systems

Note: Specific wording in the nSpect tool should be viewed as a starting point for selecting the applicability of the risk item to the site being inspected. Team Leads are expected to use the information provided here for each risk item and the principal of due diligence in determining the point value to assess for each risk item.

3.2 Risk Indicator Items

3.2.1 Unique Findings

This section of the Risk Indicator will use the same algorithm used in Continuous Monitoring and Risk Scoring (CMRS). However, CMRS will apply the algorithm on a larger scale. To condition organizations to this pending scoring system, the Risk Indicator uses the same system and applies it to all the Cat I, II and III findings reported on each network inspected during the CCRI. Only the unique numbers of findings are scored and the vulnerability scan results are used. At this time, Information Assurance Vulnerability Management (IAVM) and Non-IAVM Cat I findings (unique) are scored separately in order to provide a degree of awareness as to IAVM compliance. The CMRS algorithm is that Cat I findings (unique) are multiplied by 10, Cat IIs (unique) by 4 and Cat IIIs (unique) by 1. The Team Lead need only enter the correct number for each category of findings and the nSpect tool will calculate the correct score for this item.

3.2.2 Traditional and Network Security

Five Traditional and Network Security Cat I findings are highlighted in this section of the Risk Indicator. In light of the emphasis on Insider Threat vulnerabilities, these findings are deemed extremely important and point to significant risks. The number of instances of these Cat I findings are not enumerated. That is to say any one instance of these issues equates to a thousand point entry in the Risk Indicator. The Traditional and Network reviewers can report these Risk Indicator items to the Team Lead. Possible outcomes for this Risk Indicator item are as follows:

- Unprotected network connections (port security) and/or presence of unauthorized wireless. 1000 points.

- Classified material NOT properly handled or vaults/secure rooms NOT

meeting standards. 500 points.

- Protected Distribution System is in use without proper approval. 750 points.

3.2.3 Anti-Virus

The systems processing information on a network must be protected from malicious code at all times and that protection must be current. The scale below is intended to highlight the value of this concept and impart a value to that facet of the organization's compliance with DoD standards. A finding in this area can be from vulnerability scanning or from reviews conducted by an inspector on a specific system. The number of instances of these findings is not deemed relevant. A single finding meeting the criteria below will result in an increased Risk Indicator score. Only the most severe of the findings is scored if there are two or more findings of this nature. Possible outcomes for this Risk Indicator item are as follows:

- Antivirus definition/signature file > 23 days old. 1000 points.
- Antivirus definition/signature file is 8-23 days old. 500 points.
- Antivirus definition/signature file <= 7 days old. Zero points.

3.2.4 Host Based Security System (HBSS), ePO Server version

HBSS is a key component of computer network defense and a key element in the Risk Indicator. This item in the Risk Indicator focuses on version of the ePO server, a key management piece of this technology. The version of the ePO server is relevant from a risk perspective even if the site does not manage the ePO server.

The Defense Information Systems Agency (DISA), at the request of the United States Strategic Command (USSTRATCOM) and in support of National Security goals established by the President, has purchased from industry, a capability that will develop and deploy an automated Host-Based Security System (HBSS) solution(s) that will provide network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems.

HBSS is a collection of flexible, commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) applications. The system can detect and counter, in real-time, against known cyber threats to the Department of Defense (DoD) Enterprise. The HBSS solution will be active on each applicable host (server, desktop, and laptop) in the DoD. The system will be managed by local

administrators and configured to block known-bad traffic using an Intrusion Prevention System (IPS) and host firewall. DISA's Mission Assurance Directorate provides program management and supports the deployment of this solution. The scope of the HBSS deployment is worldwide. DISA Mission Assurance Directorate has instituted support services to enable the comprehensive implementation of the HBSS system to all the combatant commands, Services, agencies and field activities (CC/S/A/FA).

The HBSS inspector evaluating Operational Order (OPORD) 12-1016 will provide information for the Team Lead to select the correct option to evaluate this item. Possible outcomes for this Risk Indicator item are as follows:

- HBSS is not implemented. 1000 points.
- HBBS is implemented but the latest version and maintenance release of HBSS ePO server is NOT being used. 500 points.
- Latest version and maintenance release of HBSS ePO server IS being used. Zero points.

3.2.5 HBSS Endpoint Protection Components

HBSS Endpoint Protection Components consist of those agents checked in OPORD 12-1016. Currently these components are: McAfee Agent, Antivirus/Antispyware, Device Control Module (a subset of the McAfee product Data Loss Prevention), Host Intrusion Prevention System and Policy Auditor. In order to take advantage of the capability of the ePO server and current policy initiatives as part of the government's continuous development of HBSS enforced by that server, the point products or agents themselves must be of the version required by the OPORD. The HBSS inspector evaluating OPORD 12- 1016 will provide information for the Team Lead to select the correct option to evaluate this item. Note: One instance of an agent which is not current is enough to identify this condition as a risk. Possible outcomes for this Risk Indicator item are as follows:

- Any of the following HBSS Point Products are NOT in use: Host Intrusion Protection System (HIPS), McAfee Agent, Policy Auditor, Device Control Module, and Antivirus/Antispyware. 1000 points.
- Any of the following HBSS Point Products are in use but not the latest version: Host Intrusion Protection System (HIPS), McAfee Agent, Policy Auditor, Device Control Module, and Antivirus/Antispyware. 500 points.

- ALL of the following HBSS Point Products are in use with the latest version: Host Intrusion Protection System (HIPS), McAfee Agent, Policy Auditor, Device Control Module, and Antivirus/Antispyware. Zero points.

3.2.6 Continuity of Operations Plan (COOP) or equivalent

Failure to develop a COOP and test it periodically can result in the partial or total loss of operations and information security (INFOSEC). A contingency plan is necessary to reduce mission impact in the event of system compromise or disaster. In some organizations the COOP is referred to as the Business Continuity Plan. COOPs need to be tailored to the criticality level of the organization and its mission. The CCRI Contributing Factors has a check for the COOP and whether or not it has been exercised. As this is the minimum standard, it does not address the risk of attempting a recovery action which is not prioritized in any manner. This is a risk situation which could readily result in a chaotic recovery event. No credit is given to a site that has adhered to this criteria as all too often the requirement to exercise the COOP is met via a table top exercise. For Risk Indicator purposes, emphasis is placed upon the requirement to categorize a site's systems in a hierarchy – or prioritize the recovery process. This is meant to be an incentive for the site to identify its most important systems for both remediation efforts and recovery priorities. If a site does not require a COOP, this circumstance must be documented to reflect DAA knowledge of such a situation. The Traditional Reviewer can report this Risk Indicator item to the Team Lead. Possible outcomes for this Risk Indicator item are as follows:

- Site does not have a COOP or has a COOP and only exercises it via a table top exercise or the COOP is incomplete. 1000 points.

- Has a COOP plan and exercises it. Plan prioritizes recovery IAW criticality level for mission critical assets. 500 points.

- Has a COOP plan and exercises it. Plan prioritizes recovery IAW criticality level for mission critical assets. Has redundant resources or a contract and/or agreement in place to support execution of the COOP plan (e.g. vendors, contractors). Zero points.

3.2.7 Computer Network Defense Service Provider (CNDSP) Alignment and Relationship

Being correctly aligned with and leveraging the capabilities of a certified Tier II CNDSP is a requirement for all DoD organizations. The site should be able to produce a signed and current Service Level Agreement (SLA) or a Memorandum of Agreement (MOA) between itself and a Tier II CNDSP. Someone at the site should be designated the primary POC for communication with the CNDSP. This person should be conversant in the Category of incidents used by CNDSP, hold

regular meetings to resolve CNDSP reported data and appropriate follow-up actions. The site must be aware of CNDSP incident categories. The Team Lead is responsible for evaluating this Risk Indicator item. Possible outcomes for this Risk Indicator item are as follows:

- Is NOT aligned with a CNDSP or there is a CNDSP with SLA/MOA but no evidence of an interactive dialogue exists. Existence of an MOA alone is not evidence of dialogue. Look for emails or a log. 1000 points.

- Is aligned to a CNDSP with SLA/MOA and there is evidence of an interactive dialogue. POC identified with emails or log book records. 500 points.

- Is aligned to a CNDSP with SLA/MOA and there is evidence of on-going, active interaction via a site process for resolving CNDSP alerts, has an awareness of CNDSP incident categories and dialogue between site and CNDSP. Zero points.

3.2.8 Cyber Security Practices or Information Assurance Awareness

Successful protection of Department of Defense (DoD) assets requires policy compliance and an understanding of the vulnerabilities humans face when interacting with information systems. Employee awareness is a countermeasure against those vulnerabilities and a means to reduce human-related risks. To maximize the protection of systems and information, it is essential to maintain a workforce that is aware of, trained on, and educated about cyber security and assurance. Employee awareness training topics cover a broad spectrum of IA education. Examples of this training (areas where incidents could occur) are the following:

- Basic principles of information assurance
- Information accessibility, handling, labeling, and storage protection
- Physical, operational, and environmental information security protection
- Privacy Act and Personally Identifiable Information (PII) protection
- Common information security threats, vulnerabilities, and risks

This risk item recognizes that the personal behavior of system users is a significant and constant risk. The site ISSM/IAM should have a record of any security incidents in the organization being inspected -- which meets the criteria for this Risk Indicator item. Incidents initiated by another organization which are merely reported by the site being evaluated are not relevant to the site's IA awareness incident rating. The Team Lead, with input from the entire CCRI team, is responsible for evaluating this Risk Indicator item. Possible outcomes for this Risk Indicator item are as follows:

- There have been IA incidents within last 3 months (spillage, mishandled classified, email phishing incident, USB or wireless violations). 1000 points

- There have been IA incidents within last 6 months (spillage, mishandled classified, email phishing incident, USB or wireless violations). 500 points.

- There have been NO IA incidents within last 6 months (spillage, mishandled classified, email phishing incident, USB or wireless violations identified). Zero Points.

3.2.9 Dated Cat I Findings

A common theme that emerges from reports of a cyber security breach is that the breach is often related to the failure to correct a well-publicized vulnerability. Permitting vulnerabilities of Cat I severity to persist on a network for an extended period of time is most detrimental to a sound Computer Network Defense posture. Any inspector may report a dated IAVM from their technology review. Additionally, long standing Cat I STIG vulnerabilities which are reported would also be considered Dated Findings. The Team Lead is responsible for evaluating this Risk Indicator item. Possible outcomes for this Risk Indicator item are as follows:

- Excluding the CCRI vulnerability scan, there are open Cat Is older than 6 months. 1000 points.

- Excluding the CCRI vulnerability scan, there are open Cat Is less than 6 months old. 500 points.

- Excluding the CCRI vulnerability scan, there are no open Cat Is. Zero points.

3.2.10 Cross Domain Solutions (CDS)

A cross-domain solution (CDS) is a means of information assurance that provides the ability to manually or automatically access or transfer information between two or more differing security domains. They are integrated systems of hardware and software that enable transfer of information among incompatible security domains or levels of classification. Modern military, intelligence, and law enforcement operations critically depend on timely sharing of information. CDS development, assessment, and deployment are based on risk management. CDSs are considered High-Risk systems and their deployment is controlled at a high level within DoD. Thus the mere presence of a CDS in an organization is a risk factor.

The three primary elements demanded from cross domain solutions are:

- Data confidentiality: most often imposed by hardware-enforced one-way data transfer
- Data integrity: content management using filtering for viruses and malware; content examination utilities in the case of formatted data
- Data availability: role-based administration access

The inspection team may conduct the Joint Vulnerability Assessment Program (JVAP) or JVAP Administrative checks or if available a technical checklist review or a Security Test and Evaluation (ST&E) on a CDS or suite of CDS equipment.

The Team Lead is responsible for evaluating this Risk Indicator item. Possible outcomes for this Risk Indicator item are as follows:

- Any CDS is present with ANY findings of any category. 1000 points.
- Any CDS is present but there are NO findings. 500 points.
- There is no CDS present. Zero points.

3.2.11 Operational Readiness Inspections (ORI) and Exercises (ORE)

The purpose of an ORI/ORE is to validate the mission readiness of units and their ability to execute assigned missions and tasks against a defined standard. In simple terms, higher headquarters wants to validate and grade the organization's ability to safely function while following appropriate Service or higher headquarters' policy and guidance. During an ORI/ORE inspectors will introduce scenarios such as changed Force Protection levels, announce security breaches, virus threats or system outages. The goal is for the site to conduct scenarios which challenge its computer network defense procedures and processes via such inspections or exercises. The Team Lead is responsible for evaluating this Risk Indicator item by interviewing the site's leadership. Possible outcomes for this Risk Indicator item are as follows:

- No Network Defense element is included in Operational Readiness Inspections, Sea Trials (work-ups), and/or Exercises. 1000 points.
- No Network Defense element is included in Operational Readiness Inspections, Sea Trials (work-ups), and/or Exercises, HOWEVER during

these events, organization does test degraded bandwidth and/or network connectivity. 500 points.

- Network Defense element is included in Operational Readiness Inspections, Sea Trials (work-ups), and/or Exercises such as external network assessments, penetration testing, phishing exercises/tests, sensor testing and reports, incident handling). (Team Lead will capture and report examples of these activities.). Zero points.

3.2.12 Target Value for Threat Vectors

Targeted cyber security threats represent the greatest challenge to information security. The stakes are high and involve the potential for financial loss, the compromise of sensitive and personal information, public embarrassment and impact on mission accomplishment. Because a threat actor will select their target and marshal the resources needed to launch a sustained campaign against that target, security leaders and security analysts must be constantly aware of the opportunity their network and systems represents to a threat actor (i.e., adversary). This is perhaps the most challenging risk indicator item for the Team Lead to evaluate. The broad categories for targets given in the criteria below are only guidelines. The Team Lead must bring to bear his or her knowledge of the organization's mission combined with his or her awareness of real world threat activity which may be aimed at the site being inspected (i.e., NMCI sites). Cleared Defense Contractor (CDC) sites supporting sensitive PM/PORs are viewed as at least equal to command and control centers or a higher headquarters. The Team Lead is responsible for evaluating this Risk Indicator item. Possible outcomes for this Risk Indicator item are as follows:

- Flagship or Capital Ships of the USN, TNOSC, COCOM HQ, Exec Office of the President, Three letter agencies. 1000 points.

- Key Command and Control Centers, Division, Wing HQ, Service defined. 750 points.

- All others. 500 points.

3.2.13 Presence of Vulnerable Program Managed Systems

Program Managed (PM) Systems or Programs of Record (POR) have, for a variety of reasons, a reputation of non-compliance. As a result, when subjected to a vulnerability scan, results are often poor or the CCRI team learns that PM systems are not being scanned correctly. As of CCRI Phase III, the results of this scan have been rolled up into the overall grade for the vulnerability scan for the site being inspected. While this has placed increasing emphasis on the need for both the program office and the site to improve the security posture of Program Managed systems, the results of the scan for a single or small number of program

managed systems are often diluted by the scan results from a large and well-managed network. Thus, to keep focus on the risks posed by program managed systems, they are highlighted as a separate risk item. The Team Lead is responsible for evaluating this Risk Indicator item based on the concern indicator for Program Managed systems scan results (Note: If multiple PM/POR systems are scanned, select the highest concern level for evaluating this Risk Indicator item). Possible outcomes for this Risk Indicator item are as follows:

- "Critical Concern" for any one PM/POR system(s) (from scan results) or a PM system could not be scanned due to lack of credentials. 1000 points.
- “Moderate Concern" for any one PM/POR system(s) (from scan results). 750 points.
- "Minor Concern" for any one PM/POR system(s) (from scan results). 500 Points.
- No PM/POR systems present or a concern indicator(s) for PM/POR scan(s) of “No Concern”. Zero points.

3.2.14 Presence of End of Life Systems

"**End-of-life**" (**EOL**) is a term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life (from the vendor's point of view) and a vendor intends to stop marketing, selling, or sustaining it. In the computing field, the concept of EOL has significance in the production, supportability, and purchase of software, firmware and hardware products. Depending on the vendor, EOL may differ from end of service life, which has the added distinction that a vendor of systems or software will no longer provide maintenance, troubleshooting, or other support. New threats, the next generation of malware and virus technologies, will be difficult for EOL systems to deal with -- even with a Customer Support Agreement. One avenue of attack will be a new generation of Advanced Persistent Threats (APTs), which are targeted attacks focused on EOL endpoints or users that attackers perceive to be vulnerable. The Team Lead is responsible for evaluating this Risk Indicator item based on input from the CCRI team and his or her own observations during the CCRI. Current examples of EOL systems are Windows XP, CISCO IOS Release 15.0(1) SE, and soon Windows Server 2003. The former DoD scanning tool, Retina, is also considered an EOL for purposes of this Risk Indicator item. The security posture of the EOL system is not relevant. Possible outcomes for this Risk Indicator item are as follows:

- Found software, firmware, or hardware on the network which is no longer supported by the vendor. 1000 points.

- Found software, firmware, or hardware on the network and proof of extended support from an authorized source/vendor. 500 points.

- No unsupported software, firmware, or hardware on the network. Zero Points.

3.2.15 Port Security

Without port security protections in place, unauthorized devices could access a network through open and unprotected switch interfaces. The Port Security feature is used to restrict traffic on a switch interface (also called a "switch port" or "port") by identifying and limiting traffic allowed to enter that port. 802.1X is the ‘Gold’ standard for Port-based Network Access Control (PNAC) and has been required by the network STIG since 2008. In the past port-based security based upon a device’s Media Access Control, MAC, address has been permitted. However, such protection today is compromised by ‘spoofing’ MAC addresses or ‘mirroring’ MAC addresses. Such mitigations are deemed a risk which is no longer acceptable.

Not all devices support 802.1X authentication. Examples include network printers, Ethernet-based electronics like environmental sensors, cameras, and wireless phones. For those devices to be used in a protected network environment alternative mechanisms must be provided to authenticate them. One option would be to disable 802.1X on that port, but that leaves that port unprotected and open for abuse. In such cases the use the MAC Authentication Bypass or MAB option is encouraged. When MAB is configured on a port that port will first try to check if the connected device is 802.1X compliant, and if no reaction is received from the connected device, it will try to authenticate with the AAA server using the connected device's MAC address as username and password. The network administrator then must make provisions on the RADIUS server to authenticate those MAC-addresses, either by adding them as regular users, or implementing additional logic to resolve them in a network inventory database.

- 802.1x Port-based Network Access Control is not implemented on the network. 1000 points.

- MAC Authentication Bypass, MAB, Network Access Control is implemented on devices not capable of 802.1X authentication. 500 points.

- 802.1x Port-based Network Access Control is implemented on the network. Zero Points.

3.2.16 Configuration Management

Configuration management, CM, is a management discipline that is applied over the life cycle of a product or information system to provide visibility and control of its functional and physical characteristics. Benefits of configuration management include:

- Accounting of hardware and software inventories
- Tracking system/environment configurations
- Maintaining network topology diagrams
- Maintaining Information Assurance (IA) documentation
- Making approved changes to system configurations or documentation at the approved time and in the approved manner

The focus of this check is to follow up on the Contributing Factor, 2.12, Configuration Management Process Indicator "Evidence that the Configuration Management Process is enforced".

During the conduct of the CCRI should the CCRI team observe the site not following its own CM process this is indicative of imposing an element of risk in the site's IT assets. A common example is the introduction of configuration statements used for a test or exercise which are then not removed until they are identified by the CCRI inspection process. The risk can be characterized as evidence of a lack of control over the site's management of its IT resources.

- Configuration changes are observed or reported by the site without being subjected to the site's CM process (i.e., changes made on the fly or stating during the hot-wash that a change was made by the SA or Network Engineer on the spot). 1000 points.

- Site does not have an 'urgent or expedited' configuration management process which authorizes rapid changes to system configurations. 500 points.

- No violations of the site's configuration management process were observed during the CCRI. Zero Points.

3.3 Risk Indicator Score Exception

This case is the only instance in which the CCRI score directly impacts the Risk Indicator score or outcome. Whenever the CCRI score is less than 70.0% (an unacceptable grade) the risk indicator will automatically be adjusted to indicate the network in question is a High Risk to the DoDIN. The intent is to capture the risk

inherent in a failed CCRI outcome. In some cases the risk indicator items scored may not reflect a root cause for the failed grade as the Risk Indicator items being evaluated may not capture the Culture, Capability and Conduct issues which contributed to the failed CCRI outcome. Again, to adequately capture the risk associated with such circumstances, the risk to the DoDIN from a network evaluated as Unacceptable will automatically be listed as High.

APPENDIX A: RISK REPORTING GUIDE

General

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 rev 1, **Guide for Conducting Risk Assessments,** details the risk assessment process and the approach outlined in this document has been adapted to the CCRI program.

Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the **likelihood** of occurrence. Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. *Risk assessment* is the process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur.

Risk Assessment is the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

Risk assessments are a key part of effective risk management and facilitate decision making at all three tiers in the risk management hierarchy. These tiers are the organization level, mission/business process level, and the information system level. Because risk management is ongoing, risk assessments are conducted throughout the system development life cycle. However, from the perspective of the CCRI, the focus is on risks associated with the sustainment (i.e., operations/support) phase of the life cycle. Risk assessments are not simply one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security risks. Rather, organizations employ risk assessments on an ongoing basis throughout the system development life cycle and across all of the tiers in the risk management hierarchy.

In Phase IV of the CCRI the requirement for a Risk Assessment and After Action Plan deliverable from the site being inspected has been combined into one deliverable due no later 45 Calendar days after the CCRI Out-Brief. This combined deliverable is to be titled the Risk Report. This report will address all findings contained in the CCRI Compliance Report as well as addressing the items identified in the Risk Indicator. The purpose of the Risk Report is to identify a course of action to address all findings reported in CCRI Compliance Report as well as mitigations for items identified in the Risk Indicator. A Risk Report is required for each network inspected.

In this context, the Risk Report strives to identify:

- an organizations key IT assets. An inventory of all IT assets should be placed in order of priority as they relate to mission accomplishment.
- threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation;
- vulnerabilities internal and external to organizations (i.e., Organizational vulnerabilities are not confined to information systems but can include, for example, vulnerabilities in governance structures, mission/business processes, enterprise architecture, information security architecture, facilities, equipment, system development life cycle processes, supply chain activities, and external service providers.);
- the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and
- the likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

Furthermore, it is recognized that risk assessments are often not precise instruments of measurement and reflect the:

- limitations of the specific assessment methodologies, tools, and techniques employed;
- subjectivity (i.e., Likelihood values) and trustworthiness of the data used;
- interpretation of assessment results; and
- skills and expertise of those individuals or groups conducting the assessments.

Methodology Recommendations

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 rev 1, **Guide for Conducting Risk Assessments,** details the risk assessment process and that approach is recommended. The service cyber components have also been active in screening and directing the format and content of the Risk Assessments required from the site as a CCRI follow-up deliverable.

Risk Indicator – the Next Step

The primary reason for the Risk Indicator is to assist the organization in preparing a useful Risk Assessment. The Risk Indicator was never intended to be linked to the CCRI outcome, which is a CCRI score and grade. The Risk Indicator is intended to be aligned with the scoring system used in Continuous Monitoring and Risk Scoring, CMRS.

Per NIST 800-30 Rev 1, Risk Management Guide for Information Technology Systems, the organization conducting a Risk Assessment, must review its IT assets to determine the assets most critical to mission accomplishment. Next it must determine the vulnerabilities that exists in its environment – this is the focus of the Risk Indicator. Finally, the organization must evaluate the likelihood of the vulnerability being exploited as the vulnerability applies to its IT assets. The likelihood of exploitation is in turn tied to an awareness and understanding of the threat. Sources of threat information can vary from that available in the public domain to classified sources obtained exclusively by the organization via its service cyber organization.

The resulting evaluation can be complex and take the form of:

Vulnerability -> Threat -> IT Asset -> Exploit Likelihood -> Mission Impact
Vulnerability area/item (from Risk Indicator) -> Threat Intelligence -> IT Asset (Priority determined by site) -> Exploit Likelihood (High, Medium, Low as determined by site IT and Operations staff) -> Mission Impact = (High, Medium, Low as determined by site IT and Operations staff)

Example (1):

Situation: Site has a Cross Domain Solution, but no ATC. Risk Indicator for this vulnerability is **High**.

Vulnerability area/item (from Risk Indicator) **High** -> Threat Intelligence – **None** -> IT Asset (Priority determined by site) **High** -> Exploit Likelihood (High, Medium, Low as determined by site IT and Operations staff) **Low** -> Mission Impact = (High, Medium, Low as determined by site IT and Operations staff), **Medium** – Action: correct ATC issue.

Repeat the above process for each vulnerability and each key IT asset.

The Risk Report

The essential elements of information described here are informative and exemplary only and are not intended to require or promote a specific template for documenting risk assessment results. Organizations have flexibility in determining the type and the level of detail of information included in organizational risk assessments and the associated reports. The essential elements of information for communicating risk assessment results can be modified accordingly to meet the needs of organizations conducting the assessments.

Executive Summary

• Date of the risk assessment.
• Summarize the purpose of the risk assessment.
• Describe the scope of the risk assessment.

- For Tier 1 and Tier 2 risk assessments, identify: organizational governance structures or processes associated with the assessment (e.g., risk executive [function], budget process, acquisition process, systems engineering process, enterprise architecture, information security architecture, organizational missions/business functions, mission/business processes, information systems supporting the mission/business processes).
- For Tier 3 risk assessments, identify: the information system name and location(s), security categorization, and information system (i.e., authorization) boundary.

• State whether this is an initial or subsequent risk assessment. If a subsequent risk assessment, state the circumstances that prompted the update and include a reference to the previous Risk Assessment Report.
• Describe the overall level of risk as Low, Medium or High.

Body of the Report

• Describe the purpose of the risk assessment, including questions to be answered by the assessment. For example:

- How the use of a specific information technology would potentially change the risk to organizational missions/business functions if employed in information systems supporting those missions/business functions; or
- How the risk assessment results are to be used in the context of the RMF (e.g., an initial risk assessment to be used in tailoring security control baselines and/or to guide and inform other decisions and serve as a starting point for subsequent risk assessments; subsequent risk assessment to incorporate results of security control assessments and inform authorization decisions; subsequent risk assessment to support the analysis of alternative courses of action for risk responses; subsequent risk assessment based on risk monitoring to identify new threats or vulnerabilities; subsequent risk assessments to incorporate knowledge gained from incidents or attacks).

• Identify assumptions and constraints.
• If applicable, identify and describe the risk model and analytic approach; provide a reference or include as an appendix, identifying risk factors, value scales, and algorithms for combining values.

- Describe the uncertainties within the risk assessment process and how those uncertainties influence decisions.
- If the risk assessment includes organizational missions/business functions, describe the missions/functions (e.g., mission/business processes supporting the missions/functions, interconnections and dependencies among related missions/business functions, and information technology that supports the missions/business functions).
- If the risk assessment includes organizational information systems, describe the systems (e.g., missions/business functions the system is supporting, information flows to/from the systems, and dependencies on other systems, shared services, or common infrastructures).
- Summarize risk assessment results (e.g., using tables or graphs), in a form that enables decision makers to quickly understand the risk (e.g., number of threat events for different combinations of likelihood and impact, the relative proportion of threat events at different risk levels).
- Identify the time frame for which the risk assessment is valid (i.e., time frame for which the assessment is intended to support decisions).
- List the risks due to adversarial threats.
- List the risks due to non-adversarial threats.

APPENDIX B: ACRONYMS

AD	Active Directory
ALT	Alt-token (ALT)
ATC	Authority to Connect
CAC	Common Access Card
CAM	Coordinated Alert Messages
Cat I	Category One (vulnerability finding)
CCMD	Combatant Command
CCRI	Command Cyber Readiness Inspection
CDC	Cleared Defense Contractor
CDM	Continuous Diagnostics and Mitigation
CDS	Cross Domain Solution
CIO	Chief Information Officer
CMRS	Continuous Monitoring and Risk Scoring
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COOP	Continuity of Operations Plan
COTS	Commercial off-the-shelf
CRM	Cyber Security Risk Management
CTO	Communications Tasking Order
DoD	Department of Defense

ePO	Policy Orchestrator (enterprise, McAfee trade name)
FRAGO	Fragmentary Orders
GOTS	Government off-the-shelf
HBSS	Host-Based Security System
IAM	Information Assurance Manager
IAVM	Information Alert Vulnerability Management
IAW	In Accordance With
INFOSEC	Information Security
ISSM	Information Systems Security Manager
JVAP	Joint Vulnerability Assessment Program
MAC	Mission Assurance Category
MOA	Memorandum of Agreement
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
OGS	Operation Gladiator Shield
OPORD	Operation Order
ORE	Operational Readiness Exercise
ORI	Operational Readiness Inspection
PIV	Personal Identify Verification
PKE	Public Key Encryption
PM	Program Managed (systems)
POR	Programs of Record (systems)
SIPRNet	SECRET Internet Protocol Router Network

SLA	Service Level Agreement
SP	Special Publication
ST&E	Security Test & Evaluation
STIG	Secure Technical Implementation Guide
TASKORD	Task Order
TL	Team Lead
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
WARNORD	Warning Orders